

HEURISTICS FOR ANTI-CYCLOTOMIC \mathbb{Z}_p -EXTENSIONS

DEBANJANA KUNDU AND LAWRENCE C. WASHINGTON

ABSTRACT. This paper studies Iwasawa invariants in anti-cyclotomic towers. We do this by proposing two heuristics supported by computations. First we propose the *Intersection Heuristics*: these model ‘how often’ the p -Hilbert class field of an imaginary quadratic field intersects the anti-cyclotomic tower and to what extent. Second we propose the *Invariants Heuristics*: these predict that the Iwasawa invariants λ and μ usually vanish for imaginary quadratic fields.

1. INTRODUCTION

Let K be a number field and let p be a prime, which we shall always take to be odd. Let K_∞/K be a \mathbb{Z}_p -extension, which means $\text{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$, the additive group of p -adic integers. Let K_n be the subfield of degree p^n over K , let h_n be its class number, and let p^{e_n} be the exact power of p dividing h_n . A well-known result of K. Iwasawa says there exist integers $\lambda, \mu \geq 0$ and ν , independent of n , such that

$$e_n = \lambda n + \mu p^n + \nu,$$

for all n sufficiently large.

When K is an imaginary quadratic field, there are two exactly \mathbb{Z}_p -extensions such that K_∞/\mathbb{Q} is a Galois extension. One is the *cyclotomic* \mathbb{Z}_p -extension K_{cyc}/K : this is contained in the field obtained by adjoining all p -power roots of unity to K and is such that $\text{Gal}(K_{\text{cyc}}/\mathbb{Q})$ is abelian. The other is the *anti-cyclotomic* \mathbb{Z}_p -extension K_{ac}/K and is such that $\text{Gal}(K_{\text{ac}}/\mathbb{Q})$ is dihedral, with $\text{Gal}(K/\mathbb{Q})$ acting on $\text{Gal}(K_{\text{ac}}/K)$ by inversion.

The μ -invariant for K_{cyc} is always 0 (see [FW79]), and the distribution of λ -invariants when p is fixed and K varies has been studied by several authors, see for example [San91, DFKS91, Oza01, Fuj13, Mur19]. In [EJV11], J. Ellenberg–S. Jain–A. Venkatesh studied this question in the special case when K varies over all imaginary quadratic fields and p is non-split in K ; they proposed a heuristic based on random p -adic matrices. These heuristics have recently been extended to abelian extensions by D. Delbourgo–H. Knospe in [DK22]. The initial goal of our study was to see if similar predictions could be made for K_{ac} . However, our calculations suggest that K_{ac}/K where p is non-split in K acts more like the cyclotomic \mathbb{Z}_p -extensions of totally real number fields, where Greenberg’s Conjecture (see [Gre76]) predicts that $\mu = \lambda = 0$.

Let $L(K)$ be the p -Hilbert class field of K , that is, the maximal unramified abelian p -extension of K . Then $\text{Gal}(L(K)/K)$ is isomorphic to A_0 , the Sylow p -subgroup of the ideal class group of K . A phenomenon that plays a prominent role when studying anti-cyclotomic \mathbb{Z}_p -extensions is that $L(K) \cap K_{\text{ac}}$ can be larger than K . The question is how large can this intersection be? Based on computational evidence, we propose the following:

Date: June 5, 2023.

2020 *Mathematics Subject Classification.* Primary 11R23.

Conjecture (Intersection Heuristics). *Fix a finite abelian p -group G . Let K vary over imaginary quadratic fields such that p is non-split in K and the p -part of its ideal class group is isomorphic to G . The probability that $L(K) \cap K_{\text{ac}} = K_n$ is given by*

$$\frac{\#(\text{elements of } G \text{ of order exactly } p^n)}{\#G}.$$

This number is also

$$\frac{\#(\text{homomorphisms } G \longrightarrow \mathbb{Q}/\mathbb{Z} \text{ with image of size } p^n)}{\#G}.$$

In other words, the p -class group G randomly maps to $\text{Gal}(K_n/K)$ for large n and the frequency of possible images is predicted to model the distribution of possible intersections.

The Cohen-Lenstra heuristics (introduced in [CL90]) predict that the p -part of the ideal class group of K is most often cyclic, and our heuristic says that for cyclic G , it is most common that $L(K)$ is contained in K_{ac} . A result of S. Fujii (see Theorem 2.2) says that $\mu = \lambda = 0$ in this case. Moreover, our calculations suggest that $\mu = 0$ is always true, and that $\lambda = 0$ when A_0 is cyclic and $L(K) \cap K_{\text{ac}} = K$. Putting these together yields the following:

Conjecture (Invariants Heuristics). *Among the imaginary quadratic fields K in which p does not split, we always have $\mu = 0$, and the proportion for which $\lambda = 0$ is at least*

$$\left(1 - \frac{1}{p}\right) + \frac{1}{p-1} \prod_{j \geq 1} (1 - p^{-j}).$$

For $p = 3$, this predicts that $\lambda = 0$ at least 94% of the time, and for $p = 5$ at least 99% of the time. These are heuristic lower bounds, but we find it hard to imagine that there is such a small number of actual exceptions. Therefore we ask the following:

Question. *Is $\lambda = \mu = 0$ always true for the anti-cyclotomic \mathbb{Z}_p -extension of an imaginary quadratic field K in which p does not split?*

We restrict ourselves to the case that p does *not* split in K because in the complementary case it is known that $\lambda > 0$. This follows from a result of [Oza01] (see for example [Fuj13, p. 283]).

Another situation where there is possibly an analogue of Greenberg's conjecture was considered in [FK02]. Suppose p splits in K as $\mathfrak{p}\bar{\mathfrak{p}}$. Let K_∞/K be the \mathbb{Z}_p -extension in which only \mathfrak{p} ramifies and assume it is totally ramified. It is known that $\mu = 0$ (see [Gil87, Sch87]), and the computations in [FK02] suggest that also $\lambda = 0$.

For cyclotomic \mathbb{Z}_p -extensions of imaginary quadratic fields, R. Gold was able to evaluate the λ -invariant from the class numbers of the first few levels, see [Gol74]. We have followed a similar strategy in our situation but it is more challenging. In the cyclotomic case, Gold used the fact that the inverse limit of the p -class groups has no finite submodules. This is no longer the case for anti-cyclotomic \mathbb{Z}_p -extensions, as can be seen from the several cases where $\lambda = \mu = 0$ but $\nu > 0$. Consequently, our methods cannot recognize situations where $\lambda > 0$ or $\mu > 0$, if they exist.

In addition to proposing the above heuristics, we prove the following result (see Theorem 6.1) which asserts that the Sylow p -subgroup of the ideal class group of the n -th layer of the anti-cyclotomic extension, denoted by A_n , is non-cyclic if A_0 is non-trivial and disjoint from K_{ac} .

Theorem. *Let K be an imaginary quadratic field and let p be an odd prime that does not split in K . Suppose that A_0 is non-trivial. If the p -Hilbert class field of K is disjoint from K_{ac} , then A_n is non-cyclic for all $n \geq 1$.*

Organization: Including this Introduction, the article has seven sections. In Section 2, we record facts from classical Iwasawa theory and remind the reader of the Cohen–Lenstra heuristics. In Section 3, we consider the case when the p -Hilbert class field of K is disjoint from the anti-cyclotomic tower. We present data and prove sufficient conditions for the Iwasawa invariants to be trivial. In Section 4, we study the case when the p -Hilbert class field partially intersects the anti-cyclotomic tower. The computational methods for obtaining the tables in the above sections are explained in Section 5. In Section 6, we prove that in the case that the p -Hilbert class field of K is disjoint from the anti-cyclotomic tower, the p -Hilbert class field of each subsequent layer K_n must be non-cyclic. Finally, in Section 7 we present the two heuristics and explain the rationale behind them. The **Intersection Heuristics** model ‘how often’ the p -Hilbert class field intersects the anti-cyclotomic tower and ‘how much’ is the intersection. The **Invariants Heuristics** aim to predict ‘how often’ the anti-cyclotomic Iwasawa invariants are trivial.

2. PRELIMINARIES

2.1. Anti-cyclotomic Iwasawa theory. Let K be an imaginary quadratic field and p be a fixed prime. There exists a Galois extension \tilde{K}/K containing all the \mathbb{Z}_p -extensions of K such that

$$\mathrm{Gal}(\tilde{K}/K) \simeq \mathbb{Z}_p^2.$$

This 2-dimensional Galois extension contains uncountably many quotients isomorphic to \mathbb{Z}_p , and each quotient corresponds to some \mathbb{Z}_p -extension K_∞/K . There are two \mathbb{Z}_p -extensions that are special because they are the only ones that are Galois over \mathbb{Q} . One is the often-studied *cyclotomic* \mathbb{Z}_p -extension which is abelian over \mathbb{Q} ; the other is the *anti-cyclotomic* \mathbb{Z}_p -extension, denoted by K_{ac} , which is a pro-dihedral group (and hence non-abelian).

Lemma 2.1. *Keep the same notations as introduced above. Then,*

$$L(K) \cap \tilde{K} \subseteq K_{\mathrm{ac}}.$$

Proof. For a proof of this assertion, we refer the reader to [Fuj13, Lemma 2.2]. \square

In view of the above lemma, the following three situations may arise:

- (a) $L(K) \cap K_{\mathrm{ac}} = L(K)$, i.e., the p -Hilbert class field of K is contained in K_{ac} .
- (b) $L(K) \cap K_{\mathrm{ac}} = K$, i.e., the p -Hilbert class field of K is disjoint from K_{ac} .
- (c) $K \subsetneq L(K) \cap K_{\mathrm{ac}} \subsetneq L(K)$, i.e., the p -Hilbert class field of K partially intersects K_{ac} .

The following theorem shows that the Iwasawa invariants in case (a) are well understood.

Theorem 2.2. *With notation as introduced above, if $L(K) \subsetneq K_{\mathrm{ac}}$ then*

$$\mu(K_{\mathrm{ac}}/K) = \lambda(K_{\mathrm{ac}}/K) = 0.$$

Proof. This assertion is proved in [Fuj13, Remarks on p. 286] using Chevalley’s formula. \square

2.2. Cohen–Lenstra Heuristics. The Cohen–Lenstra heuristics are based on the observation that structures often occur in nature with frequency inversely proportional to their number of automorphisms. The idea of the Cohen–Lenstra heuristics is that the p -part of the ideal class group of K (with $p \neq 2$) is a finite abelian p -group that is distributed in this way.

Cohen–Lenstra Heuristics. Let $D^-(x)$ denote the set of imaginary quadratic fields K such that $|\text{Disc } K| \leq x$ and let $G(n)$ denote the set of all finite groups of order n . For any ‘reasonable’ function f on finite abelian groups,

$$\lim_{x \rightarrow \infty} \frac{\sum_{K \in D^-(x)} |f(\text{Cl}(K))|}{\#\{K \in D^-(x)\}} = \lim_{n \rightarrow \infty} \frac{\sum_{i=1}^n \sum_{G \in G(i)} \frac{f(G)}{\#\text{Aut}(G)}}{\sum_{i=1}^n \sum_{G \in G(i)} \frac{1}{\#\text{Aut}(G)}}.$$

The main examples where these heuristics are applied are when f depends on the Sylow p -subgroup of G .

3. DATA AND INITIAL CALCULATIONS: p -HILBERT CLASS FIELD IS DISJOINT FROM K_{ac}

In this section, we consider the case where the p -Hilbert class field of K is disjoint from K_{ac} . For computational reasons, we restrict to $p = 3$ (when $p = 5$, the extension K_2/\mathbb{Q} has degree 50, and it is hard to compute class numbers of fields of such a large degree). The methods of computation are described in Section 5.

3.1. Data for the case that A_0 is cyclic. Calculations presented in the data below were performed using PARI/GP. In these tables, we record the p -part of the ideal class group in the first few layers of the anti-cyclotomic \mathbb{Z}_p -extension of $K = \mathbb{Q}(\sqrt{-d})$. Here, A_n is the Sylow p -subgroup of the ideal class group of K_n . To keep the tables less cumbersome, we write n in place of $\mathbb{Z}/n\mathbb{Z}$. Since the p -Hilbert class field of K is disjoint from K_{ac} , it follows that the unique prime above p is totally ramified in the anti-cyclotomic \mathbb{Z}_p -extension. First, in Table 1 we consider the case when 3 is inert in the imaginary quadratic field. In Table 2 we present the data when 3 ramifies in the imaginary quadratic field.

TABLE 1. 3 is inert

d	A_0	A_1	A_2	d	A_0	A_1	A_2
331	3	$3 \times 3 \times 3$	$3 \times 3 \times 3 \times 3$	2491	3	3×3	3×3
643	3	3×3	3×3	2740	3	3×3	3×3
835	3	3×3	3×3	2791	3	3×3	3×3
1048	3	27×9	27×27	2824	3	3×3	3×3
1192	3	3×3	3×3	2923	3	3×3	3×3
1327	3	3×3	3×3	2344	9	9×3	9×9
1588	3	3×3	3×3	3643	9	9×3	9×9
1843	3	27×9	81×27	4819	9	9×3	9×9
1951	3	3×3	3×3	5464	9	9×3	9×9
2227	3	$3 \times 3 \times 3$	$3 \times 3 \times 3 \times 3$	6763	9	9×3	9×9
2488	3	3×3	3×3				

TABLE 2. 3 is ramified

d	A_0	A_1	A_2	d	A_0	A_1	A_2
804	3	3×3	3×3	3540	3	3×3	3×3
1236	3	3×3	3×3	3912	3	3×3	3×3
1272	3	3×3	3×3	4308	3	3×3	3×3
1668	3	3×3	3×3	8331	9	9×3	9×9
2856	3	9×9	9×9	15243	9	9×3	9×9
3048	3	9×9	9×9	24207	9	9×3	9×9

Theorem 3.1. *In all examples in Tables 1 and 2, we have $\mu(K_{\text{ac}}/K) = 0$. For all cases except possibly $d = 1843$ and $d = 141412$, we have $\lambda(K_{\text{ac}}/K) = 0$.*

Proof. When K_{ac}/K is totally ramified, [San91, Lemma, p. 672] asserts that

$$(1) \quad \#A_n \geq \#A_0 \cdot p^{\mu(p^n-1) + \min(p^n-1, \lambda)}$$

for each $n \geq 0$. In all of the examples, we observe that

$$\#A_2 < \#A_0 \times 3^8.$$

Therefore, $\mu(K_{\text{ac}}/K) = 0$. The proofs that $\lambda(K_{\text{ac}}/K) = 0$ for these examples will be given in Sections 3.2 and 3.3. \square

3.2. Conditions for triviality of Iwasawa invariants. In this section, we provide sufficient conditions to prove that the anti-cyclotomic Iwasawa μ and λ -invariants are 0. Throughout this section we assume that K is an imaginary quadratic field, there exists exactly one ramified prime in the \mathbb{Z}_p -extension K_∞/K , and it is totally ramified. In particular, the results we prove hold when the p -Hilbert class field of K is disjoint from K_{ac} .

3.2.1. We begin by recording some results that we use several times for proving our statements. These results are true for *general* \mathbb{Z}_p -extensions, not just the anti-cyclotomic one, and they apply to arbitrary number fields K .

Lemma 3.2. *Suppose that there exists exactly one ramified prime in the \mathbb{Z}_p -extension K_∞/K ; further suppose that it is totally ramified. Set $G_n = \text{Gal}(K_{n+1}/K_n) = \langle \tau_n \rangle$. Then*

$$\#A_{n+1}^{G_n} = \#A_n.$$

Proof. This follows from Chevalley's formula; see [Ger77, Lemma 4.2]. \square

Theorem 3.3 ([Ger77, Theorem 1.3(c)]). *Suppose that there exists exactly one ramified prime in the \mathbb{Z}_p -extension K_∞/K ; further suppose that it is totally ramified. If every ideal class in A_0 becomes trivial in some A_n , then*

$$\lambda(K_\infty/K) = \mu(K_\infty/K) = 0.$$

The norm map from A_{n+1} to A_n is surjective since we are assuming throughout that K_{n+1}/K_n is totally ramified. The composition of this with the natural map from A_n to A_{n+1} yields

$$(2) \quad \begin{aligned} A_{n+1} &\longrightarrow A_{n+1} \\ [J] &\mapsto (1 + \tau_n + \dots + \tau_n^{p-1})[J]. \end{aligned}$$

Proposition 3.4. *Suppose that there exists exactly one ramified prime in the \mathbb{Z}_p -extension K_∞/K ; further suppose that it is totally ramified. Suppose that $A_n \simeq A_{n+1}$ for some $n \geq 0$. Then $\lambda(K_\infty/K) = \mu(K_\infty/K) = 0$.*

Proof. Write $L = \bigcup_{n \geq 0} L(K_n)$ and $X = \text{Gal}(L/K_\infty)$. Since there is a unique prime above p in K and this prime is totally ramified we know that (see [Was97, Proposition 13.22])

$$A_n = X / \left((1 + T)^{p^n} - 1 \right) X.$$

Since we are assuming that $A_n = A_{n+1}$, therefore

$$X / \left((1 + T)^{p^n} - 1 \right) X = X / \left((1 + T)^{p^{n+1}} - 1 \right) X.$$

Nakayama's Lemma now implies that $\left((1 + T)^{p^n} - 1 \right) X = 0$; therefore, X must be finite. \square

Remark 3.5. This proposition allows us to take care of, for example, the cases $d = 2856$ and 3048 in Table 2.

Proposition 3.6. *Suppose that there exists exactly one ramified prime in the \mathbb{Z}_p -extension K_∞/K ; further suppose that it is totally ramified. Suppose that for some n both A_n and A_{n+1} are elementary p -groups satisfying*

$$\text{rank}_p(A_{n+1}) \leq \text{rank}_p(A_n) + p - 2.$$

Then $\lambda(K_\infty/K) = \mu(K_\infty/K) = 0$.

Proof. Write τ_n for a generator of $\text{Gal}(K_{n+1}/K_n) = G_n$. By Lemma 3.2, $\#A_{n+1}^{G_n} = \#A_n$.

Consider A_{n+1} as a vector space over \mathbb{F}_p and τ_n as a linear transformation such that $\tau_n^p = 1$. Note that 1 is the only eigenvalue of τ_n .

The assumption on ranks implies that the 1-eigenspace of τ_n has codimension $\leq p - 2$. If we now look at the Jordan form of τ_n , then no Jordan block has size larger than $p - 1$. Write

$$\tau_n = I + N \text{ satisfying } N^{p-1} = 0.$$

Hence,

$$(3) \quad \begin{aligned} 1 + \tau_n + \dots + \tau_n^{p-1} &= I + (I + N) + (I + N)^2 + \dots + (I + N)^{p-1} \\ &= pI + \sum_{k=1}^{p-1} \sum_{j=1}^{p-2} \binom{k}{j} N^j. \end{aligned}$$

Observe that for a fixed $j \leq p - 2$,

$$\sum_{k=1}^{p-1} \binom{k}{j} = \sum_{k=j}^{p-1} \binom{k}{j} = \binom{p}{j+1} \equiv 0 \pmod{p}.$$

Putting this all together we rewrite (3) as follows:

$$1 + \tau_n + \dots + \tau_n^{p-1} \equiv 0 \pmod{p}.$$

In particular, the map given in (2) is a multiple of p . By assumption, A_{n+1} is an elementary p -group; hence it is annihilated under this map. But, the norm map is surjective; hence we conclude that $A_n \rightarrow A_{n+1}$ is the 0-map. By Theorem 3.3 the result follows. \square

Proposition 3.7. *Suppose that there exists exactly one ramified prime in the \mathbb{Z}_p -extension K_∞/K ; further suppose that it is totally ramified. Suppose that*

$$A_0 \simeq \mathbb{Z}/p^2\mathbb{Z}, \quad A_1 = \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, \quad A_2 = \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}.$$

Then,

$$\lambda(K_\infty/K) = \mu(K_\infty/K) = 0.$$

Proof. The elements of A_1 can be written as column vectors $\begin{pmatrix} x \\ y \end{pmatrix}$ with $x \in \mathbb{Z}/p^2\mathbb{Z}$ and $y \in \mathbb{Z}/p\mathbb{Z}$.

Let τ_1 be a generator for $\text{Gal}(K_1/K) = G$. The action of τ_1 on A_1 is via the matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that

$$\tau_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix} \quad \text{and} \quad \tau_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} b \\ d \end{pmatrix}.$$

Since $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ is an element of order p , it forces that $b \equiv 0 \pmod{p}$.

By Lemma 3.2, we know that

$$A_1^G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \text{ or } A_1^G \simeq \mathbb{Z}/p^2\mathbb{Z}.$$

We claim that in both cases, $1 + \tau_1 + \tau_1^2 + \dots + \tau_1^{p-2} = p$.

Case 1 – $A_1^G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$: We may choose the fixed elements of A_1 to be the column vectors $\begin{pmatrix} p \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and this forces

$$M = \begin{pmatrix} a & 0 \\ c & 1 \end{pmatrix} \text{ such that } a \equiv 1 \pmod{p}.$$

Note that for $0 \leq j \leq p-1$,

$$M^j = \begin{pmatrix} a^j & 0 \\ \sum_{i=0}^{j-1} a^i c & 1 \end{pmatrix} = \begin{pmatrix} a^j & 0 \\ jc & 1 \end{pmatrix}$$

since $a \equiv 1 \pmod{p}$. Therefore, we calculate that

$$I + M + \dots + M^{p-1} = pI.$$

Case 2 – $A_1^G \simeq \mathbb{Z}/p^2\mathbb{Z}$: There is a fixed column vector of order p^2 and we may choose

$$M = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}.$$

Since $M^p = I$, this forces $d = 1$. Note that for $0 \leq j \leq p-1$,

$$M^j = \begin{pmatrix} 1 & jb \\ 0 & 1 \end{pmatrix}.$$

Therefore, we obtain that

$$I + M + \dots + M^{p-1} = pI.$$

Continuing with the proof, let $[J_0]$ be an ideal class in A_0 and $[J_1]$ be an ideal class in A_1 satisfying

$$\mathbf{N}_{K_1/K}([J_1]) = [J_0].$$

Here we have used the fact that $\mathbf{N}_{K_1/K}$ is surjective since the extension is totally ramified. On the other hand, the image of $\mathbf{N}_{K_1/K}[J_1] = [J_0]$ in A_1 is

$$(I + M + \dots + M^{p-1})[J_1] = p[J_1].$$

Suppose that $\langle \tau_2 \rangle = \text{Gal}(K_2/K_1) = G_2$ and $A_2 \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$. The action of τ_2 on A_2 can be understood via an invertible 2×2 matrix M_2 with coefficients in $\mathbb{Z}/p^2\mathbb{Z}$. Lemma 3.2 implies that there are fixed column vectors of order p^2 and order p , which we choose to be $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ p \end{pmatrix}$, respectively. Therefore, we choose

$$M_2 = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \text{ with } b \equiv 0 \pmod{p} \text{ and } d \equiv 1 \pmod{p}.$$

Note that once again for $0 \leq j \leq p-1$,

$$M_2^j = \begin{pmatrix} 1 & \sum_{i=0}^{j-1} bd^i \\ 0 & d^j \end{pmatrix} = \begin{pmatrix} 1 & jb \\ 0 & d^j \end{pmatrix}.$$

Therefore, we obtain that

$$I + M + \dots + M^{p-1} = pI.$$

Working with the class $[J_1]$ from before, we know there exists a class $[J_2]$ in A_2 such that

$$[J_1] = \mathbf{N}_{K_2/K}[J_2].$$

As before, $[J_1] \mapsto p[J_2]$ in K_2 . Therefore,

$$[J_0] \mapsto p[J_1] \mapsto p^2[J_2] = 0.$$

The result follows from Theorem 3.3. □

Remark 3.8.

- (i) Theorem 3.1 and Propositions 3.6 and 3.7 show that $\lambda(K_{\text{ac}}/K) = \mu(K_{\text{ac}}/K) = 0$ for all imaginary quadratic fields considered in Tables 1 and 2 except when $d = 1048$ or 1843 .
- (ii) The above propositions do not apply to the case $d = 1048$. However, the prime above 7 generates A_0 and this prime becomes principal in A_2 . By Theorem 3.3, we know that

$$\lambda(K_{\text{ac}}/K) = \mu(K_{\text{ac}}/K) = 0.$$

- (iii) Now, consider the case $d = 1843$. The prime above 11 generates A_0 but it does not become principal in A_2 . So, we can not draw such a conclusion. The result of Sands mentioned in the proof of Theorem 3.1 implies that $\lambda \leq 6$. It appears possible in this case that $\lambda(K_{\text{ac}}/K) = 2$. But, it is perhaps unlikely that this is an exceptional case where $\lambda(K_{\text{ac}}/K) > 0$; we have not yet been able to compute the image of A_0 in A_3 .

3.3. Data for the case that A_0 is non-cyclic. Here are a few cases where A_0 is non-cyclic and the 3-Hilbert class field is disjoint from K_{ac} .

TABLE 3. A_0 is non-cyclic

d	A_0	A_1	A_2
50983	3×3	$9 \times 3 \times 3 \times 3$	$9 \times 9 \times 3 \times 3$
63079	3×3	$9 \times 3 \times 3 \times 3$	$9 \times 9 \times 3 \times 3$
141412	3×3	$9 \times 3 \times 3 \times 3$	$27 \times 9 \times 3 \times 3$

The results proven in Section 3.2 can not be applied to these examples. Here, we do not prove general results but only comment on these specific examples.

- (a) In each of these cases, $\mu(K_{\text{ac}}/K) = 0$ by the same argument as in Theorem 3.1.
(b) When $d = 50983$, the 10th powers of the primes above 13 and 23 generate A_0 . They both become principal in A_2 . Theorem 3.3 implies that

$$\mu(K_{\text{ac}}/K) = \lambda(K_{\text{ac}}/K) = 0.$$

- (c) When $d = 63079$, the 17th powers of the primes above 5 and 41 generate A_0 . They both become principal in A_2 . Once again, Theorem 3.3 implies that

$$\mu(K_{\text{ac}}/K) = \lambda(K_{\text{ac}}/K) = 0.$$

- (d) When $d = 141412$, the 8th powers of the primes above 7 and 43 generate A_0 . The 8th-power of the prime above 43 becomes principal in A_2 but the 8th-power of the prime above 7 has order 3 in A_2 . Therefore, we do not draw any conclusions regarding the λ -invariant from this. The result of Sands mentioned in the proof of Theorem 3.1 implies that $\lambda(K_{\text{ac}}/K) \leq 5$.

4. DATA AND CALCULATIONS: p -HILBERT CLASS FIELD PARTIALLY INTERSECTS K_{ac}

In this section, we first present the table where the p -Hilbert class field partially intersects K_{ac} .

TABLE 4. p -Hilbert class field of K intersects with K_{ac} partially

d	A_0	A_1	A_2	d	A_0	A_1	A_2
367	9	3	9×3	6883	9	3	9×3
1087	9	3	9×3	7908	9	3	9×3
1291	9	3	9×3	13092	9	3	9×3
3547	9	3	$3 \times 3 \times 3 \times 3$	36276	3×3	$3 \times 3 \times 3$	$9 \times 9 \times 9 \times 3$
4012	9	3	9×3	49128	3×3	9×3	27×9
6607	9	3	9×3	49812	3×3	9×3	27×9
6871	9	3	9×3	58920	3×3	9×3	27×9

In this next proposition we provide a proof of an observation one is likely to make immediately from the above table. As before, write $L(K_n)$ to denote the p -Hilbert class field of K_n .

Proposition 4.1. *Suppose that A_0 is cyclic and $L(K) \supseteq K_n$ for some $n \geq 0$. Then $L(K_n) = L(K)$.*

Proof. Note that $L(K) \subseteq L(K_n)$. Suppose that $L(K) \neq L(K_n)$, then

$$1 \neq \text{Gal}(L(K_n)/L(K)) \trianglelefteq \text{Gal}(L(K_n)/K).$$

Since these are p -groups there exists an index p subgroup N of $\text{Gal}(L(K_n)/L(K))$ that is normal in $\text{Gal}(L(K_n)/K)$, see [DF04, Section 6.1, Theorem 1(3)]. Consider the exact sequence

$$1 \longrightarrow \text{Gal}(L(K_n)/L(K)) / N \longrightarrow \text{Gal}(L(K_n)/K) / N \longrightarrow A_0 \longrightarrow 1.$$

By hypothesis, A_0 is cyclic and it acts on $\text{Gal}(L(K_n)/L(K)) / N$, by lifting and then conjugation. However, $\text{Gal}(L(K_n)/L(K)) / N$ has order p which means that there are no automorphisms of order p . The action of A_0 must therefore be trivial. Hence, $\text{Gal}(L(K_n)/K) / N$ is abelian. Write F for the number field fixed by N . We have the following tower of number fields:

$$K \subseteq K_n \subseteq L(K) \subsetneq F \subseteq L(K_n).$$

This means that F/K is abelian and unramified but this contradicts the assumption that $L(K)$ is the p -Hilbert class field. \square

Remark 4.2.

- (i) This proposition does not hold when A_0 is non-cyclic, as we can see from the data.
- (ii) It seems to be difficult to make any accurate predictions about the anti-cyclotomic Iwasawa invariants from this data. For $d \neq 36276$, the result of Sands mentioned in the proof of Theorem 3.1, applied to K_2/K_1 , says that $\mu(K_{\text{ac}}/K) \leq 1$, and if $\mu(K_{\text{ac}}/K) = 1$ then $\lambda(K_{\text{ac}}/K) = 0$. For $d = 36276$, we find that $\mu(K_{\text{ac}}/K) \leq 2$, and if $\mu(K_{\text{ac}}/K) = 2$ then $\lambda(K_{\text{ac}}/K) = 0$.

5. COMPUTATIONAL METHODS I

We now explain how the computations were performed to obtain data for the p -part of the ideal class groups of the first few layers of the anti-cyclotomic tower in the earlier sections. Our techniques are a modification of those of [BHW19].

5.1. Let z be an element in the upper half plane and define

$$\eta(z) = q^{1/24} \prod_{n \geq 1} (1 - q^n) \text{ where } q = e^{2\pi iz}.$$

Define the *Weber functions*

$$f(z) = e^{-\pi i/24} \frac{\eta\left(\frac{z+1}{2}\right)}{\eta(z)} \text{ and } f_1(z) = \frac{\eta\left(\frac{z}{2}\right)}{\eta(z)}.$$

The following result of R. Schertz [Sch02, Theorem 1] plays a crucial role in our computations.

Schertz's Theorem. *Let α be an element in the upper half plane satisfying the primitive equation*

$$AX^2 + BX + C = 0 \text{ with } 2 \nmid A \text{ and } B \equiv 0 \pmod{32}$$

with discriminant $D = B^2 - 4AC = -4m = -t^2d$. Then, each of the following numbers generates the ring class of conductor t over the imaginary quadratic field of discriminant $-d$ in the case stated:

- $\left(\left(\frac{2}{A}\right) \frac{1}{\sqrt{2}} f(\alpha)^2\right)^3$ if $m \equiv 1 \pmod{8}$.
- $f(\alpha)^3$ if $m \equiv 3 \pmod{8}$.
- $\left(\frac{1}{2} f(\alpha)^4\right)^3$ if $m \equiv 5 \pmod{8}$.
- $\left(\left(\frac{2}{A}\right) \frac{1}{\sqrt{2}} f(\alpha)\right)^3$ if $m \equiv 7 \pmod{8}$.
- $\left(\left(\frac{2}{A}\right) \frac{1}{\sqrt{2}} f_1(\alpha)^2\right)^3$ if $m \equiv 2, 6 \pmod{8}$.
- $\left(\left(\frac{2}{A}\right) \frac{1}{2\sqrt{2}} f_1(\alpha)^2\right)^3$ if $m \equiv 4 \pmod{8}$.

Here, $\left(\frac{2}{A}\right)$ denotes the Legendre symbol.

Let $\alpha_1, \alpha_2, \dots, \alpha_{h_t}$ be the roots corresponding to the set of all classes of conductor t (satisfying the conditions that the coefficient A_i is odd and $32 \mid B_i$), and let g be one of the above expressions. Then $\{g(\alpha_i)\}_i$ gives a complete set of conjugates of $g(\alpha_1)$ over the imaginary quadratic field of discriminant $-d$.

Start with a primitive quadratic form

$$ax^2 + bxy + cy^2 \text{ with } b^2 - 4ac = -4m.$$

If $2 \mid a$, we perform the change of variables $y \mapsto (x + y)$ and obtain

$$(a + b + c)x^2 + (b + 2c)xy + cy^2.$$

Note that $2 \mid b$ and the original quadratic form is primitive. Thus, c and $a + b + c$ are both odd. Next, suppose we have the quadratic form

$$a_1x^2 + b_1xy + c_1y^2 \text{ with } 2 \nmid a_1.$$

Choose m satisfying

$$b_1 + 2a_1m \equiv 0 \pmod{32}.$$

Perform the change of variable $x \mapsto x + my$. This gives the quadratic form

$$a_1x^2 + (b_1 + 2a_1m)xy + (c_1 + mb_1 + m^2a_1)y^2.$$

Therefore, each class of quadratic forms is represented as a primitive quadratic form $Ax^2 + Bxy + Cy^2$ with $2 \nmid A$ and $32 \mid B$.

Let α be the root in the upper half plane of $Ax^2 + Bx + C = 0$. Compute the value of the appropriate function $g(\alpha)$ from [Schertz's Theorem](#). This number generates the ring class field over $K = \mathbb{Q}(\sqrt{-d})$. The minimal polynomial of $g(\alpha)$ over \mathbb{Q} has roots $g(\alpha_1), \dots, g(\alpha_{h_t})$.

For our study, we need polynomials that generate a layer of the anti-cyclotomic \mathbb{Z}_p -extension of K . Such a layer will be contained in a ring class field of conductor 9^k for some k . To use [Schertz's Theorem](#), multiply d by 4 (if required) and by a power p^{2k} to get $-4m$. For k sufficiently large, compute the group of reduced primitive quadratic forms of discriminant $-4m$, call it G . Choose an integer M and let H be the subgroup of G consisting of elements of G whose orders divide M . An appropriate choice of M makes G/H cyclic of order a power of p . The integer M in our calculations was essentially the class number of K times a power of 2 and a power of 3.

Define the polynomial

$$\prod_{aH \in G/H} \left(x - \sum_{h \in H} g(\alpha_{ah}) \right);$$

here g is the function in [Schertz's Theorem](#) and α_{ah} is the element of the upper half plane corresponding to the quadratic form ah . Observe that $\sum_{h \in H} g(\alpha_{ah})$ is the trace to the fixed field of H ; the roots of the polynomial must lie in this field, which is cyclic over K and of degree a power of p . In all the cases that were considered, these roots generated the field and the polynomial has rational integral coefficients. From the structure of the ring class group (and since we removed the elements of order dividing the class number of K), we know that cyclic p -power extensions obtained in the manner explained above is a layer of the anti-cyclotomic \mathbb{Z}_p -extension.

Remark 5.1. The calculations were done in floating point (often to 10000- or 20000-digit accuracy for the larger discriminants) and then rounded to get a polynomial with integer coefficients (the many-digit accuracy was needed in order to make the rounding well-defined; PARI/GP keeps track of this). The polynomial generating the compositum of K with the field generated by a root of the polynomial yields a polynomial generating the layer of the \mathbb{Z}_p -extension over K . As a check, the discriminant of the number field was computed and it always had the correct prime factors to the correct powers. As the power p^{2k} increases, we get higher layers of the \mathbb{Z}_p -extension.

5.2. We now give a concrete example. Let $d = 1048$, $p = 3$, and $K = \mathbb{Q}(\sqrt{-1048})$, which has class number 6. Note that $d/4 = 262 \equiv 6 \pmod{8}$ so $g(\alpha) = \left(\left(\frac{2}{A} \right) \frac{1}{\sqrt{2}} f_1(\alpha)^2 \right)^3$.

Let G be the group of reduced primitive quadratic forms of discriminant -1048×9^k for $k = 3, 4$ and H be the subgroup of forms of order dividing 24. When $k = 3$, we have $\#G = 216$ and $\#H = 72$. Therefore, we get a polynomial of degree 3. The command `polredbest` in PARI/GP reduces this polynomial to one with smaller coefficients that generates the same field, namely

$$x^3 + 42x - 40.$$

This polynomial generates the first layer K_1/K . The polynomial that generates K_1/\mathbb{Q} is given by

$$x^6 - 90x^4 - 56x^3 + 4383x^2 + 4092x + 1046.$$

When $k = 4$, $\#G = 648$ and $\#H = 72$. The degree 9 polynomial we obtain is

$$x^9 - 99x^7 - 414x^6 - 2025x^5 + 13086x^4 + 396855x^3 + 830250x^2 + 1026756x - 2776392.$$

Finally, the degree 18 polynomial that generates K_2/\mathbb{Q} is given by

$$\begin{aligned} x^{18} - 2970x^{14} - 13080x^{12} + 7331265x^{10} + 259656840x^8 + 3345463512x^6 \\ + 18497139840x^4 + 129166770960x^2 + 1140995344768. \end{aligned}$$

6. NON-CYCLICITY OF A_n WHEN A_0 IS DISJOINT FROM K_{ac}

Recall that in Section 3 we considered the case that the p -Hilbert class field of K is non-trivial and completely disjoint from the anti-cyclotomic tower. The data in Tables 1 and 2 seem to indicate that A_1 and A_2 are non-cyclic. In this section, we prove this observation.

Theorem 6.1. *Let K be an imaginary quadratic field and let p be an odd prime that does not split in K . Suppose that A_0 is non-trivial. If the p -Hilbert class field of K is disjoint from K_{ac} , then A_n is non-cyclic for all $n \geq 1$.*

The proof will occupy the remainder of this section. Let A_n denote the Sylow p -subgroup of the ideal class group of K_n . Since K_n/K_0 is totally ramified, the norm map

$$A_n \longrightarrow A_0$$

Remark 6.2. In the case that $p = 3$, we are assuming that $A_0 \simeq \mathbb{Z}/3^u\mathbb{Z}$. It follows that we need not worry about the special case when $p = 3$ and $K = \mathbb{Q}(\sqrt{-3})$, where $A_0 = 1$. Therefore, throughout our discussion, we have the additional property that \mathcal{O}_K^\times has order prime to p .

$$(4) \quad \#A_1^G = \frac{\#A_0 \times p}{p[\mathcal{O}_K^\times : \mathcal{O}_K^\times \cap \mathbf{N}_{K_1/K}(K_1^\times)]} = \#A_0.$$

Proof. Suppose that $\#A_1 = \#A_0$. It follows from (4) that $A_1 = A_1^G$.

$$I^\tau = I\alpha \text{ for some } \alpha \in K_1.$$
$$(1) = \left(\mathbf{N}_{K_1/K}(\alpha) \right).$$
$$\alpha = \beta^{1-\tau} \text{ for some } \beta \in K_1.$$
$$(I\beta)^\tau = I\beta.$$
$$\begin{array}{ccc}
L(K) \cdot K_1 & & \\
\downarrow & \searrow & \\
L(K) & & K_1 \\
\downarrow & \searrow & \downarrow \\
A_0 & & K \\
& & \downarrow \\
& & \mathbb{O}
\end{array}
\quad \begin{array}{c} \\ \\ \\ \text{Z/pZ} \\ \\ \end{array}$$

By hypothesis there is a unique prime $\mathfrak{p} \mid p$ in K that ramifies in K_1 . Denote by \mathfrak{P} this unique prime above p in K_1 . Recall that a prime splits completely in the p -Hilbert class field if and only if its ideal class has order prime to p . For a non-split prime $\mathfrak{p} \mid p$, we know that either \mathfrak{p} or \mathfrak{p}^2 is principal in K . Therefore, the ideal class has order 1 or 2. It follows that \mathfrak{p} splits completely in $L(K)/K$. Note that $\mathfrak{P} \mid p$ splits completely in $L(K) \cdot K_1/K_1$. We have assumed that $\#A_1 = \#A_0$, so we conclude that $L(K) \cdot K_1 = L(K_1)$ (since K_1/K_0 is a ramified extension). Since we have shown that $\mathfrak{P} \mid p$ splits completely in $L(K_1)$, it has order prime to p in the class group of K_1 .

Again consider the ideal I . From the above discussion, we conclude that there exists an integer h' that is not divisible by p such that the class of $I^{h'}$ is represented by an ideal from A_0 . We choose h' to be the order of the prime-to- p part of the class number of K_1 . Therefore, the natural map $A_0 \rightarrow A_1$ is surjective. But, the norm map $A_1 \rightarrow A_0$ is also surjective because K_1/K is a ramified extension. This means that the composition

$$A_0 \longrightarrow A_1 \xrightarrow{N_{K_1/K}} A_0,$$

which is the p^{th} -power map must be surjective. But, this is a contradiction. \square

Lemma 6.4. *With the notation and setting as above, A_1 is not cyclic of order p^k with $k \geq u+2$.*

Proof. Claim: The extension $L(K_1)/K$ is non-abelian.

Justification: Suppose that $L(K_1)/K$ is abelian. Let \mathfrak{p} be the unique prime above p in K . The inertia group of \mathfrak{p} has order p ; so, the fixed field is an abelian unramified extension of K of degree p^k . But this contradicts the assumption that $\#A_0 = p^u$.

Recall the notation $G := \text{Gal}(K_1/K) = \langle \tau \rangle$. As a consequence of the above claim, we see that τ gives a non-trivial automorphism of A_1 of order p .

Now suppose that $A_1 \simeq \mathbb{Z}/p^k\mathbb{Z}$. Note that $\text{Aut}(A_1)$ has a unique subgroup of order p , which is generated by multiplication by $1 + p^{k-1}$. The fixed group of this subgroup has order p^{k-1} but we have observed before that $\#A_1^G = p^u$. This implies that $k = u+1$. \square

6.2. In the remainder of the discussion we will crucially require that we are studying the anti-cyclotomic \mathbb{Z}_p -extension of K . Denote by \mathcal{G} the Galois group $\text{Gal}(L(K_1)/K_0)$. Suppose that $A_1 \simeq \mathbb{Z}/p^{u+1}\mathbb{Z}$. We have the following exact sequence

$$0 \longrightarrow \mathbb{Z}/p^{u+1}\mathbb{Z} \longrightarrow \mathcal{G} \longrightarrow \langle \tau \rangle \longrightarrow 0.$$

Since τ acts on $\mathbb{Z}/p^{u+1}\mathbb{Z}$ as an automorphism of order p , we can identify

$$\langle \tau \rangle \simeq 1 + p^u\mathbb{Z}/p^{u+1}\mathbb{Z}.$$

An element $x \in 1 + p^u\mathbb{Z}/p^{u+1}\mathbb{Z}$ acts on $\mathbb{Z}/p^{u+1}\mathbb{Z}$ by multiplication by x . The group \mathcal{G} has the following concrete description

$$\mathcal{G} \simeq \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in 1 + p^u\mathbb{Z}/p^{u+1}\mathbb{Z}, b \in \mathbb{Z}/p^{u+1}\mathbb{Z} \right\}.$$

The quotient group $G = \text{Gal}(K_1/K) = \langle \tau \rangle$ is represented by matrices of the form $\begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix}$. Note that

$$\begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1/c & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & bc \\ 0 & 1 \end{pmatrix}.$$

Lemma 6.5. *With the notation introduced above,*

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & pb \\ 0 & 1 \end{pmatrix}$$

Proof. First, we rewrite

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}.$$

Therefore

$$\begin{aligned}
\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^p &= \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \times \cdots \times \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^{-1} \times \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^2 \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^{-2} \times \cdots \\
&\quad \times \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^{p-1} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^{-(p-1)} \times \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^p \\
&= \prod_{j=0}^{p-1} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^j \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^{-j} \times \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^p \\
&= \prod_{j=0}^{p-1} \begin{pmatrix} 1 & a^j b \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & \sum_{j=0}^{p-1} a^j b \\ 0 & 1 \end{pmatrix}.
\end{aligned}$$

Recall that $a = 1 + kp^u$ for some integer k . Therefore,

$$\sum_{j=0}^{p-1} a^j \equiv 1 + (1 + kp^u) + (1 + 2kp^u) + \cdots + (1 + (p-1)kp^u) \equiv p \pmod{p^{u+1}}.$$

This completes the proof of the lemma. \square

Lemma 6.6. *There is no automorphism ϕ of \mathcal{G} such that for each $a \in 1 + p^u\mathbb{Z}/p^{u+1}\mathbb{Z}$, there exists $b_a \in \mathbb{Z}/p^{u+1}\mathbb{Z}$ satisfying*

$$\phi\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} 1/a & b_a \\ 0 & 1 \end{pmatrix}.$$

Proof. We prove this by contradiction; suppose such an automorphism ϕ exists.

Consider the matrix $P = \begin{pmatrix} 1 + p^u & 0 \\ 0 & 1 \end{pmatrix}$. Then, there exists b such that

$$\phi(P) = \begin{pmatrix} 1 - p^u & b \\ 0 & 1 \end{pmatrix}.$$

Note that P has order p . Therefore, using Lemma 6.5 we see that

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 - p^u & b \\ 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & pb \\ 0 & 1 \end{pmatrix}.$$

Consequently, $b \equiv 0 \pmod{p^u}$.

Now consider the matrix $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ of order p^{u+1} . Applying the automorphism ϕ , we obtain

$$\phi(M) = \begin{pmatrix} d & e \\ 0 & 1 \end{pmatrix}$$

which must also have order p^{u+1} . Therefore,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} d & e \\ 0 & 1 \end{pmatrix}^{p^u} = \begin{pmatrix} 1 & p^u e \\ 0 & 1 \end{pmatrix}.$$

Consequently, $e \not\equiv 0 \pmod{p}$.

Finally, consider

$$(5) \quad \phi(PMP^{-1}) = \phi\left(\begin{pmatrix} 1 & 1+p^u \\ 0 & 1 \end{pmatrix}\right) = \phi(M^{p^u+1}).$$

We know that

$$\begin{aligned} \phi(PMP^{-1}) &= \phi(P)\phi(M)\phi(P^{-1}) = \begin{pmatrix} 1-p^u & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & e \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1-p^u & b \\ 0 & 1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} d & e(1-p^u) \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

For the last equality, we have used the fact that $b \equiv 0 \pmod{p^u}$ and $d \equiv 1 \pmod{p^u}$.

On the other hand

$$\begin{aligned} \phi(M^{p^u+1}) &= \phi(M)^{p^u} \phi(M) = \begin{pmatrix} d & e \\ 0 & 1 \end{pmatrix}^{p^u} \begin{pmatrix} d & e \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & p^u e \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & e \\ 0 & 1 \end{pmatrix} \quad \text{by Lemma 6.5} \\ &= \begin{pmatrix} d & e(1+p^u) \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

By (5), it follows that

$$\begin{pmatrix} d & e(1-p^u) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} d & e(1+p^u) \\ 0 & 1 \end{pmatrix}.$$

Equivalently,

$$e(1-p^u) \equiv e(1+p^u) \pmod{p^{u+1}}.$$

This contradicts the fact that $e \not\equiv 0 \pmod{p}$. This completes the proof of the lemma. \square

We now prove Theorem 6.1.

Proof. We know from the calculations done in Section 6.1 that A_1 is not cyclic of order p^u or order p^k where $k \geq u+2$. We are only left to eliminate the case that A_1 is cyclic of order p^{u+1} .

The concrete description of A_1 is as follows:

$$A_1 = \text{Gal}(L(K_1)/K_1) \simeq \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z}/p^{u+1}\mathbb{Z} \right\}.$$

Complex conjugation gives an element $\phi \in \text{Aut}(\mathcal{G})$ that maps A_1 to itself. Since K_1 is contained in K_{ac} , it means that ϕ acts by inversion on $\langle \tau \rangle$; i.e.,

$$\phi\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right) \equiv \begin{pmatrix} 1/a & 0 \\ 0 & 1 \end{pmatrix} \pmod{A_1}.$$

But, such a ϕ does not exist by Lemma 6.6. This contradicts the assumption that $A_1 \simeq \mathbb{Z}/p^{u+1}\mathbb{Z}$. This completes the proof of the theorem. \square

7. HEURISTICS

In this section, we aim to understand, as K varies over all imaginary quadratic fields, how often $L(K)$ is disjoint from K_{ac} , partially intersecting K_{ac} , and completely contained inside K_{ac} .

7.1. Fix an odd prime p . Let K be an imaginary quadratic field and K_{ac} denote the anti-cyclotomic \mathbb{Z}_p -extension of K . Let K_n denote the n -th layer of the \mathbb{Z}_p -extension, and $L(K)$ be the p -Hilbert class field of K . Write A_n to denote the p -part of the ideal class group of K_n for all $n \geq 0$.

Intersection Heuristics. *Fix a finite abelian p -group G . Let K vary over imaginary quadratic fields such that p is non-split in K and the p -part of its ideal class group is isomorphic to G . The probability that $L(K) \cap K_{\text{ac}} = K_n$ is given by*

$$\frac{\#(\text{elements of } G \text{ of order exactly } p^n)}{\#G}.$$

This number is also

$$(H1) \quad \frac{\#(\text{homomorphisms } G \longrightarrow \mathbb{Q}/\mathbb{Z} \text{ with image of size } p^n)}{\#G}.$$

In particular, we expect that as K varies over imaginary quadratic fields with $A_0 \simeq G$, the probability that class field is disjoint from K_{ac} is $\frac{1}{\#G}$.

7.1.1. As K varies over all imaginary quadratic fields, the probability that the class field is disjoint is given by

$$(6) \quad \frac{\sum_G (\text{frequency of } G)(1/\#G)}{\sum_G (\text{frequency of } G)}.$$

Set $\text{Aut}(G)$ to denote the group of all automorphisms of G . Define

$$w(p^k) = \sum_{\#G=p^k} \frac{1}{\#\text{Aut}(G)}.$$

Here, the sum is over finite abelian p -groups of order p^k .

It follows from the Cohen–Lenstra heuristics (see for example [Woo16, Proposition 5.7]) that the denominator of (6) is given by

$$\sum_G (\text{frequency of } G) = \sum_{\alpha=0}^{\infty} w(p^\alpha) = \prod_{j \geq 1} (1 - p^{-j})^{-1}.$$

On the other hand, the numerator of (6) is given by

$$\sum_G (\text{frequency of } G)(1/\#G) = \sum_{\alpha=0}^{\infty} w(p^\alpha)p^{-\alpha} = \prod_{j \geq 2} (1 - p^{-j})^{-1}.$$

Therefore, we obtain that as K varies over all imaginary quadratic number fields, the probability that the ideal class group of K is *completely disjoint* from K_{ac} is given by

$$(7) \quad \prod_{j \geq 2} (1 - p^{-j})^{-1} \times \prod_{j \geq 1} (1 - p^{-j}) = 1 - \frac{1}{p}.$$

Remark 7.1. Note that this includes those imaginary quadratic fields for which $p \nmid h_K$ and these fields are a major contribution to the total. As per the Cohen–Lenstra heuristics, varying over all imaginary quadratic fields the probability that $p \nmid h_k$ is given by

$$\prod_{j \geq 1} (1 - p^{-j}).$$

7.1.2. Let us now calculate, as K varies over all imaginary quadratic fields, the probability that the p -Hilbert class field is contained in K_{ac} . For such a K , we must have A_0 cyclic.

If G is a cyclic p -group of order p^k with $k \geq 1$, its automorphism group has order $\phi(p^k)$. Also,

$$\#(\text{surjective homomorphisms } G \rightarrow \mathbb{Z}/p^k\mathbb{Z}) = \phi(p^k).$$

As we vary over all imaginary quadratic fields K , the probability that the p -class field is (non-trivial) and *completely contained* in K_{ac} is given by

$$(8) \quad \frac{\sum_{k \geq 1, G \simeq \mathbb{Z}/p^k\mathbb{Z}} (\text{frequency of } G) \cdot \frac{\#(\text{surjective homomorphisms } G \rightarrow \mathbb{Z}/p^k\mathbb{Z})}{\#G}}{\sum_G (\text{frequency of } G)} = \left(\sum_{k \geq 1} \frac{1}{\phi(p^k)} \cdot \frac{\phi(p^k)}{p^k} \right) \prod_{j \geq 1} (1 - p^{-j}) = \frac{1}{p-1} \prod_{j \geq 1} (1 - p^{-j}).$$

7.2. In this section we predict how often $\mu(K_{\text{ac}}/K) = \lambda(K_{\text{ac}}/K) = 0$ as K varies over all imaginary quadratic fields such that p does not split.

The computational data presented in Section 3 and the results proven in Section 3.2 suggest the following: in addition to the case, where the anti-cyclotomic Iwasawa invariants are provably 0, we should expect that $\mu(K_{\text{ac}}/K) = \lambda(K_{\text{ac}}/K) = 0$ when $L(K) \cap K_{\text{ac}} = K$. The probability that the p -Hilbert class field is disjoint from the anti-cyclotomic tower was calculated in (7). On the other hand, the probability that we are in the situation considered in Theorem 2.2 is calculated in (8). Therefore, we may propose the following:

Invariants Heuristics. *Among the imaginary quadratic fields K in which p does not split,*

$$\begin{aligned} \text{Prob}(\mu(K_{\text{ac}}/K) = \lambda(K_{\text{ac}}/K) = 0) &\geq \left(1 - \frac{1}{p}\right) + \frac{1}{p-1} \prod_{j \geq 1} (1 - p^{-j}) \\ &= 1 - p^{-3} - p^{-4} - p^{-5} + p^{-7} + \dots \end{aligned}$$

7.3. **Computational Method and Data.** In this section, we provide tables which show how much of the p -Hilbert class field of K intersects with K_{ac} , when $p = 3, 5$. This provides computational evidence in support of our heuristics, at least in the case when $p = 3, 5$. Before that, we explain how the computations were done using PARI/GP.

The starting point is a special case of the following result of D. Brink [Bri07, Theorem 2].

Brink’s Theorem. *Let p be an odd prime, and K be an imaginary quadratic field of discriminant $-d$ and class number $h = p^\theta u$ (such that $\gcd(p, u) = 1$). Let $\ell \neq p$ be a prime number that splits as $\bar{\ell}$ in K , and define ν as follows:*

$$[L(K) \cap K_{\text{ac}} : K] = p^\nu.$$

Further, write

$$\ell^h = \begin{cases} a^2 + db^2 & \text{if } d \not\equiv 3 \pmod{4} \\ a^2 + ab + ((d+1)/4)b^2 & \text{if } d \equiv 3 \pmod{4} \end{cases}$$

with relatively prime $a, b \in \mathbb{Z}$. Set

$$\omega = \begin{cases} \sqrt{-d} & \text{if } d \not\equiv 3 \pmod{4} \\ (1 + \sqrt{-d})/2 & \text{if } d \equiv 3 \pmod{4} \end{cases}.$$

The following conclusions hold for $n \geq 0$.

(i) p splits in K : Write $(a + b\omega)^{p-1} = a^* + b^*\omega$. Then

$$\mathfrak{l} \text{ splits completely in } K_n \iff b^* \equiv 0 \pmod{p^{n+1+\theta-\nu}}.$$

(ii) p is inert in K : Write $(a + b\omega)^{p+1} = a^* + b^*\omega$. Then

$$\mathfrak{l} \text{ splits completely in } K_n \iff b^* \equiv 0 \pmod{p^{n+1+\theta-\nu}}.$$

(iii) p ramifies in K : If the conditions of the exceptional case (case (4) below) don't hold, then,

$$\mathfrak{l} \text{ splits completely in } K_n \iff b \equiv 0 \pmod{p^{n+\theta-\nu}}.$$

(iv) $p = 3$ and $d \equiv 3 \pmod{9}$: Write $(a + b\omega)^3 = a^* + b^*\omega$. Then

$$\mathfrak{l} \text{ splits completely in } K_n \iff b^* \equiv 0 \pmod{p^{n+2+\theta-\nu}}.$$

Corollary 7.2. Keep the notation introduced above and let v_p denote the p -adic valuation. Then,

$$\nu = \begin{cases} -1 - \theta + \min\{v_p(b^*) \mid \ell \neq p \text{ splits in } K\} & \text{if } p \text{ splits in } K. \\ -1 - \theta + \min\{v_p(b^*) \mid \ell \neq p \text{ splits in } K\} & \text{if } p \text{ is inert in } K. \\ -\theta + \min\{v_p(b) \mid \ell \neq p \text{ splits in } K\} & \text{if } p \text{ ramifies in } K \text{ but not the exceptional case.} \\ -2 - \theta + \min\{v_p(b^*) \mid \ell \neq p \text{ splits in } K\} & \text{if } p = 3 \text{ and } d \equiv 3 \pmod{9}. \end{cases}$$

The corollary follows from the case $n = 0$ of the theorem since the theorem then gives a characterization of the primes ℓ that split in K . The degree p^ν of the intersection was determined using this corollary. The fundamental discriminants $-d$ were considered in the ranges described below each table. We found the minimum over only primes $\ell < 400$ that split in K . Hence, it is possible that the counts in our tables are slightly incorrect, but not enough to affect the overall agreement with our heuristic model (7.1). The computations of the class numbers were done in PARI/GP, and therefore depend on the correctness of the Generalized Riemann Hypothesis. We assume that this also does not affect the overall agreement with the heuristic model.

How to read the tables that follow. The results are arranged according to the isomorphism class of A_0 . For example, in Table 5 in the second row, there are 31483 fields in the range mentioned such that $A_0 \simeq \mathbb{Z}/9\mathbb{Z}$. The fraction where $[L(K) \cap K_{\text{ac}} : K] = 9$ is 0.678017, the fraction where $[L(K) \cap K_{\text{ac}} : K] = 3$ is 0.213734, and the fraction where $L(K)$ is disjoint from K_{ac} is 0.108249. The row labelled ‘Expected’ gives the fractions predicted by (7.1).

TABLE 5. $d = 3k - 1$, $100,000,000 \leq k \leq 101,000,000$

A_0	Number	3^4	3^3	3^2	3	1
3	94133	0	0	0	0.674429	0.325571
Expected		0	0	0	0.666667	0.333333
9	31483	0	0	0.678017	0.213734	0.108249
Expected		0	0	0.666667	0.222222	0.111111
27	10262	0	0.678718	0.214481	0.072988	0.033814
Expected		0	0.666667	0.222222	0.074074	0.037037
81	3551	0.669107	0.227542	0.069839	0.021121	0.012391
Expected		0.666667	0.222222	0.074074	0.024691	0.012346

TABLE 6. $d = 3k + 1$, $100,000,000 \leq k \leq 101,000,000$

A_0	Number	3^4	3^3	3^2	3	1
3	93747	0	0	0	0.675328	0.324672
Expected		0	0	0	0.666667	0.333333
9	31072	0	0	0.677620	0.214663	0.107718
Expected		0	0	0.666667	0.222222	0.111111
27	10477	0	0.677770	0.216283	0.069486	0.036461
Expected		0	0.666667	0.222222	0.074074	0.037037
81	3495	0.678970	0.214306	0.072103	0.023748	0.010873
Expected		0.666667	0.222222	0.074074	0.024691	0.012346

TABLE 7. $d = 9k + 3$, $1,000,000 \leq k \leq 1,100,000$

A_0	Number	3^4	3^3	3^2	3	1
3	9298	0	0	0	0.687567	0.312433
Expected		0	0	0	0.666667	0.333333
9	2961	0	0	0.676798	0.209389	0.113813
Expected		0	0	0.666667	0.222222	0.111111
27	1103	0	0.675431	0.212149	0.074343	0.038078
Expected		0	0.666667	0.222222	0.074074	0.037037
81	350	0.717143	0.182857	0.071429	0.020000	0.008571
Expected		0.666667	0.222222	0.074074	0.024691	0.012346

TABLE 8. $d = 9k + 6$, $1,000,000 \leq k \leq 1,100,000$

A_0	Number	3^4	3^3	3^2	3	1
3	9279	0	0	0	0.692532	0.307468
Expected		0	0	0	0.666667	0.333333
9	3029	0	0	0.689006	0.206339	0.104655
Expected		0	0	0.666667	0.222222	0.111111
27	1065	0	0.712676	0.186854	0.066667	0.033803
Expected		0	0.666667	0.222222	0.074074	0.037037
81	321	0.716511	0.190031	0.059190	0.018692	0.015576
Expected		0.666667	0.222222	0.074074	0.024691	0.012346

TABLE 9. $d = 3k - 1$, $100,000,000 \leq k \leq 150,000,000$

A_0	Number	3^4	3^3	3^2	3	1
9×9	420	0	0	0.900000	0.078571	0.021429
Expected		0	0	0.888889	0.098765	0.012346
27×9	215	0	0.688372	0.297674	0.013953	0.000000
Expected		0	0.666667	0.296296	0.032922	0.004115
81×9	72	0.555556	0.333333	0.111111	0.000000	0.000000
Expected		0.666667	0.222222	0.098765	0.010974	0.001372

TABLE 10. $d = 3k + 1$, $10,000,000 \leq k \leq 100,000,000$

A_0	Number	3^2	3	1
$3 \times 3 \times 3$	597	0	0.988275	0.011725
Expected		0	0.962963	0.037037
$9 \times 3 \times 3$	287	0.728223	0.268293	0.003484
Expected		0.666667	0.320988	0.012346

TABLE 11. $d = 5k + 2$, $1,000,000 \leq k \leq 2,000,000$

A_0	Number	5^4	5^3	5^2	5	1
5	39002	0	0	0	0.802779	0.197221
Expected		0	0	0	0.800000	0.200000
25	7639	0	0	0.807566	0.154078	0.038356
Expected		0	0	0.800000	0.160000	0.040000
125	1383	0	0.806218	0.151844	0.033984	0.007954
Expected		0	0.800000	0.160000	0.032000	0.008000
625	203	0.753695	0.201970	0.044335	0.000000	0.000000
Expected		0.800000	0.160000	0.032000	0.006400	0.001600

TABLE 12. $d = 5k$, $10,000,000 \leq k \leq 20,000,000$

A_0	Number	5^3	5^2	5	1
5×5	2122	0	0	0.967484	0.032516
Expected		0	0	0.960000	0.040000
25×5	493	0	0.833671	0.164300	0.002028
Expected		0	0.800000	0.192000	0.008000
125×5	48	0.812500	0.145833	0.041667	0.000000
Expected		0.800000	0.160000	0.038400	0.001600

ACKNOWLEDGEMENTS

DK is supported by a PIMS postdoctoral fellowship.

REFERENCES

- [BHW19] Reinier Bröker, David Hubbard, and Lawrence C. Washington, *Explicit computations in Iwasawa theory*, Proceedings of the Thirteenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 2, Math. Sci. Publ., Berkeley, CA, 2019, pp. 137–153.
- [Bri07] David Brink, *Prime decomposition in the anti-cyclotomic extension*, Math. Comp. **76** (2007), no. 260, 2127–2138.
- [CL90] Henri Cohen and Hendrik Lenstra, Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983: Proceedings of the Journées arithmétiques held at Noordwijkerhout, The Netherlands, July 11–15, 1983, Springer, 1990.
- [DF04] David S Dummit and Richard Foote, *Abstract algebra*, John Wiley&Sons, 2004.
- [DFKS91] David Dummit, David Ford, Hershy Kisilevsky, and Jonathan Sands, *Computation of Iwasawa lambda invariants for imaginary quadratic fields*, J. Number Theory **37** (1991), no. 1, 100–121.
- [DK22] Daniel Delbourgo and Heiko Knospe, *On Iwasawa λ -invariants for abelian number fields and random matrix heuristics*, 2022, arXiv preprint 2207.06287.

- [EJV11] Jordan Ellenberg, Sonal Jain, and Akshay Venkatesh, *Modeling λ -invariants by p -adic random matrices*, Comm. Pure Appl. Math. **64** (2011), no. 9, 1243–1262.
- [FK02] Takashi Fukuda and Keiichi Komatsu, *Non-cyclotomic \mathbb{Z}_p -extensions of imaginary quadratic fields*, Exp. Math. **11** (2002), no. 4, 469–475.
- [Fuj13] Satoshi Fujii, *On a bound of λ and the vanishing of μ of \mathbb{Z}_p -extensions of an imaginary quadratic field*, J. Math. Soc. Japan **65** (2013), no. 1, 277–298.
- [FW79] Bruce Ferrero and Lawrence Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. Math. (1979), 377–395.
- [Ger77] Frank Gerth, *Structure of l -class groups of certain number fields and \mathbb{Z}_l -extensions*, Mathematika **24** (1977), no. 1, 16–33.
- [Gil87] Roland Gillard, *Transformation de Mellin–Leopoldt des fonctions elliptiques*, J. Number Theory **25** (1987), no. 3, 379–393.
- [Gol74] Robert Gold, *Examples of Iwasawa invariants*, Acta Arithmetica **26** (1974), no. 1, 21–32.
- [Gre76] Ralph Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), no. 1, 263–284.
- [Mur19] Kazuaki Murakami, *On an upper bound of λ -invariants of \mathbb{Z}_p -extensions over an imaginary quadratic field*, J. Math. Soc. Japan **71** (2019), no. 3, 1005–1026.
- [Oza01] Manabu Ozaki, *Iwasawa invariants of \mathbb{Z}_p -extensions over an imaginary quadratic field*, Class field theory—its centenary and prospect, Advanced Studies in Pure Mathematics **30** (2001), 387–399.
- [San91] Jonathan Sands, *On small Iwasawa invariants and imaginary quadratic fields*, Proc. Amer. Math. Soc. **112** (1991), no. 3, 671–684.
- [Sch87] Leila Schneps, *On the μ -invariant of p -adic L -functions attached to elliptic curves with complex multiplication*, J. Number Theory **25** (1987), no. 1, 20–33.
- [Sch02] Reinhard Schertz, *Weber’s class invariants revisited*, J. Théor. Nombres Bordeaux **14** (2002), no. 1, 325–343.
- [Was97] Lawrence Washington, *Introduction to cyclotomic fields*, Graduate texts in Mathematics, vol. 83, Springer, 1997.
- [Woo16] Melanie Matchett Wood, *Asymptotics for number fields and class groups*, Directions in Number Theory (Ellen Eischen, Ling Long, Rachel Pries, and Katherine Stange, eds.), Springer International Publishing, 2016, pp. 291–339.

(Kundu) DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER BC, V6T 1Z2, CANADA

Email address: dkundu@math.toronto.edu

(Washington) DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MARYLAND, COLLEGE PARK, MD 20742 USA

Email address: lcw@umd.edu