INFINITE HILBERT CLASS FIELD TOWERS FROM GALOIS REPRESENTATIONS

KIRTI JOSHI AND CAMERON McLEMAN

Abstract. We investigate class field towers of number fields obtained as fixed fields of modular representations of the absolute Galois group of the rational numbers. First, for each \( k \in \{12, 16, 18, 20, 22, 26\} \), we give explicit rational primes \( \ell \) such that the fixed field of the mod-\( \ell \) representation attached to the unique normalized cusp eigenforms of weight \( k \) on \( \text{SL}_2(\mathbb{Z}) \) has an infinite class field tower. Under a conjecture of Hardy and Littlewood, we further prove that there exist infinitely many such primes for each \( k \) (in the above list). Second, given a non-CM curve \( E/\mathbb{Q} \), we show that there exists an integer \( M_E \) such that the fixed field of the representation attached to the \( n \)-division points of \( E \) has an infinite class field tower for a set of integers \( n \) of density one among integers coprime to \( M_E \).

1. Introduction

Most current examples of number fields known to have an infinite (Hilbert) class field tower are constructed “from the bottom up,” e.g., by beginning with a fixed number field and constructing extensions of that number field in which a large number of primes ramify. If sufficiently many primes ramify, invoking results from genus theory and one of many variants of the Golod-Shafarevich inequality is enough to prove the class field tower infinite. We investigate instead class field towers of number fields obtained “from the top down,” i.e., as fixed fields of representations of the absolute Galois group \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) and prove that many naturally occurring fields of arithmetic interest have infinite Hilbert class field towers. In the process, we prove also prove, assuming a conjecture of Hardy-Littlewood, that there are infinitely cyclotomic fields of prime conductor with infinite Hilbert class field towers.

We consider two primary sources for these representations. First, we consider Galois representations arising from modular forms. For any \( k \in \{12, 16, 18, 20, 22, 26\} \), it is well-known that there exists a unique normalized cuspidal Hecke eigenform \( \Delta_k \) on \( \text{SL}_2(\mathbb{Z}) \) of weight \( k \) with integer Fourier coefficients. For each such form and rational prime \( \ell \), we consider the fixed field of the associated mod-\( \ell \) representation \( \rho_{\Delta_k, \ell} \). We find explicit examples of primes \( \ell \) such that each of these fixed fields have an infinite class field tower. The key new idea is to use certain auxiliary cubic fields introduced by Daniel Shanks (see [12]). Using these auxiliary fields and a refined Golod-Shafarevich type inequality of R. Schoof (see [8]) we show that, for suitable primes \( \ell \), the fixed fields of the mod-\( \ell \) representations alluded to earlier have an infinite Hilbert class field tower. Moreover, assuming a well-known conjecture of Hardy and Littlewood on prime values of quadratic polynomials, we prove the existence of infinitely many such \( \ell \) (see Theorem 2.3 and Corollary 2.4). Further, the fields arising from these mod-\( \ell \) representations have Galois groups containing \( \text{SL}_2(\mathbb{Z}/\ell) \) and are ramified at a single finite prime (in contrast to the number fields shown to have an infinite class field tower via genus theory). As a consequence, we also show
that the conjecture of Hardy and Littlewood implies the existence of infinitely many 
primes \( \ell \) such that the cyclotomic fields \( \mathbb{Q}(\zeta_\ell) \) have infinite Hilbert class field towers. 

For the second construction, let \( E/\mathbb{Q} \) be an elliptic curve without complex multiplica-
tion. For any \( n \geq 1 \), the absolute Galois group \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) acts on the \( n \)-torsion 
points \( E[n](\overline{\mathbb{Q}}) \cong (\mathbb{Z}/n\mathbb{Z})^2 \) of \( E \). The fixed field \( K_n \) of the kernel of the associated 
representation \( \rho_n : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}/n) \) is of significant arithmetic interest. In 
Theorem 3.1, we give an elementary proof that for almost all integers \( n \) coprime to a fixed integer \( A_E \) (almost all here means outside a set of density zero), the field \( K_n \) 
has an infinite class field tower. Further, known information about these fixed fields 
can be translated into information about the fields arising in these towers. Finally, 
we note that the construction can be made fairly explicit—in Remark 3.2, we give a 
specific example of an elliptic curve and an integer \( n \) provided by the result. 

We would like to thank William McCallum and Dinesh Thakur for comments. 

## 2. Infinite Class Field Towers from Hecke Eigenforms 

For each even integer \( k \) with \( 12 \leq k \leq 26 \) and \( k \neq 14, 24 \), there exists a unique 
normalized cuspidal Hecke eigenform on \( \text{SL}_2(\mathbb{Z}) \) of weight \( k \), which we denote here 
by \( \Delta_k \). The theorem of Deligne-Serre provides for each \( \Delta_k \) and prime \( \ell \) a Galois 
representation \( \rho_{\Delta_k,\ell} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{F}_\ell) \) which is unramified outside \( \ell \). This 
representation is the reduction modulo \( \ell \) of the \( \ell \)-adic representation associated to 
\( \Delta_k \). Let \( K_{\Delta_k,\ell} \) be the fixed field of the representation. By a well-known result of 
Serre and Swinnerton-Dyer (see [11]), for any \( \Delta_k \) and sufficiently large prime \( \ell \), the 
Galois group \( \text{Gal}(K_{\Delta_k,\ell}/\mathbb{Q}) \) is the subgroup 
\[
G_\ell = \{ g \in \text{GL}_2(\mathbb{F}_\ell) : \text{det}(g) \in (\mathbb{F}_\ell^\times)^{k-1} \}
\]
of \( \text{GL}_2(\mathbb{F}_\ell) \). Note that if \((k-1,\ell-1)=1\), we obtain \( G_\ell = \text{GL}_2(\mathbb{F}_\ell) \). The theorem 
is effective and one has a complete list of the exceptional primes: 

| \( k \) | exceptional \( \ell \) for \( \Delta_k \) |
|---|---|
| 12 | 2, 3, 5, 7, 23, 691 |
| 16 | 2, 3, 5, 7, 11, 31, 59, 3617 |
| 18 | 2, 3, 5, 7, 11, 13, 43867 |
| 20 | 2, 3, 5, 7, 11, 13, 283, 617 |
| 22 | 2, 3, 5, 7, 13, 17, 131, 593 |
| 26 | 2, 3, 5, 7, 11, 17, 19, 657931 |

The field \( K_{\Delta_k,\ell} = \overline{\mathbb{Q}}^{\Delta_k,\ell} \) certainly contains the fixed field \( \overline{\mathbb{Q}}^{\text{det}(\rho_{\Delta_k,\ell})} \) of the deter-
minant representation of \( \rho_{\Delta_k,\ell} \). This is a field which is unramified outside \( \ell \) and has 
\( (\mathbb{F}_\ell^\times)^{k-1} \) as its Galois group over \( \mathbb{Q} \). If \((k-1,\ell-1)=1\), then the Galois group has 
order \( \ell - 1 \) and the extension is unramified outside \( \ell \). By class field theory, such 
an extension corresponds to a suitable quotient of \( \mathbb{Z}_\ell^\times \). The only quotient of this 
group of order \( \ell - 1 \) is the quotient by the subgroup of \( \mathbb{Z}_\ell^\times \) consisting of \( \ell \)-adic units 
congruent to 1 mod \( \ell \), and thus the determinantal fixed field is \( \mathbb{Q}(\zeta_\ell) \). Since any 
extension of a field with an infinite class field tower itself has an infinite class field 
tower (a variant of this easy lemma is proved in the middle of the proof of Theorem 
3.1), we have proven the following: 

**Theorem 2.1.** Let \( k \in \{12, 16, 18, 20, 22, 26\} \), and let \( \ell \) be a prime such that: 

- \( \ell \) is not exceptional for \( \Delta_k \);
\begin{itemize}
  \item \((k - 1, \ell - 1) = 1;\)
  \item \(\mathbb{Q}(\zeta_\ell)\) has an infinite class field tower.
\end{itemize}

Then \(\text{Gal}(K_{\Delta_k,\ell}/\mathbb{Q}) = \text{GL}_2(\mathbb{F}_\ell)\), and \(K_{\Delta_k,\ell}\) has an infinite class field tower.

We now turn to searching for primes which satisfy the hypotheses of the theorem. As a first example, we note that the prime \(\ell = 877\) satisfies the conditions of the theorem for the Ramanujan form \(\Delta_{12}\). Namely, we have that \(\gcd(12 - 1, 877 - 1) = 1\) and that \(\ell = 877\) is not an exceptional prime for \(\Delta_{12}\), so \(\rho_{\Delta_{12},877}\) is surjective. Moreover, it is shown in [8] that \(\mathbb{Q}(\zeta_{877})\) has an infinite Hilbert class field tower. Theorem 2.1 then gives that \(K_{\Delta_{12},877}\) has an infinite class field tower.

What principally remains to do is to generalize Schoof’s argument to produce a large class of primes \(\ell\) such that \(\mathbb{Q}(\zeta_\ell)\) has an infinite class field tower. We do this below, and show that if we assume the conjecture of Hardy and Littlewood presented below, the set of such primes is in fact infinite. The conjecture arose from their famous “circle method,” and should be viewed as the quadratic analogue of Dirichlet’s Theorem on primes in arithmetic (i.e., “linear”) progressions.

**Conjecture 2.2** (Hardy-Littlewood, [5]). If \(h(x) := ax^2 + bx + c \in \mathbb{Z}[x]\) satisfies:

\begin{itemize}
  \item the quantities \(a + b\) and \(c\) are not both even;
  \item the discriminant \(D(h) := b^2 - 4ac\) is not a square;
\end{itemize}

then \(h(x)\) represents infinitely many prime values.

We now show that the conjecture implies the existence of infinitely many cyclotomic fields of prime conductor with an infinite class field tower. In contrast, most techniques used to construct infinite class field towers (note in particular Remark 3.2) provide fields with highly composite conductors.

**Theorem 2.3.** Under the assumption of Conjecture 2.2, there exist infinitely many primes \(\ell\) such that \(\mathbb{Q}(\zeta_\ell)\) has an infinite class field tower.

**Proof.** Let \(k\) be a positive integer and let \(m = 12k + 2\). Consider the cubic polynomial

\[f_m(x) = x^3 - mx^2 - (m + 3)x - 1,\]

with discriminant \((m^2 + 3m + 9)^2\). With notation as in the Hardy-Littlewood conjecture, the quadratic polynomial \(m^2 + 3m + 9 = 144k^2 + 84k + 19\) has (viewed as a polynomial in \(k\)) odd \(c\) and the non-square discriminant

\[D(144k^2 + 84k + 19) = -3888.\]

Thus, assuming the conjecture, there are infinitely many values of \(k\) for which \(m^2 + 3m + 9 =: \ell\) is prime. For the remainder of the proof, we restrict to such \(k, m,\) and \(\ell\). In this case, the splitting field \(F_m\) of \(f_m(x)\) is one of Shanks’ “simplest cubic fields,” a totally real cyclic cubic field of prime conductor \(\ell\) (see [12]). Thus \(F_m\) is the unique cubic subfield of \(\mathbb{Q}(\zeta_\ell)\). Now note that since \(m \equiv 2 \mod 12\), we have \(\ell \equiv 7 \mod 12\). Since \(\ell \equiv 1 \mod 6\), there is a unique sextic subfield of \(\mathbb{Q}(\zeta_\ell)\), which we denote by \(L_m\). Further, \(6 \nmid \frac{\ell - 1}{2}\), so \(L_m \not\subset \mathbb{Q}(\zeta_\ell)^+\) is totally imaginary. Let \(h\) be


the class number of $F_m$ and $L'_m = L_m F_m^{(1)}$, giving the following diagram of fields:

Denote by $d_2 E_K$ the 2-rank of the unit group of a number field $K$. Applying [8, Proposition 3.3] to the extension $L'_m / F_m^{(1)}$, a sufficient condition for $L'_m$ to have an infinite class field tower is that the number $\rho$ of ramified primes in this extension satisfies

$$\rho \geq 3 + d_2 E_{F_m^{(1)}} + 2 \sqrt{d_2 E_{L'_m} + 1}.$$ 

Since $L'_m$ is totally imaginary and $F_m^{(1)}$ is totally real, Dirichlet’s Unit theorem easily calculates the right-hand side of this inequality to be $3 + 3 h + 2 \sqrt{3 h + 1}$. Now we count ramified primes: First, all $3 h$ infinite places of $F_m^{(1)}$ ramify in $L'_m$. Second, since $L_m / F_m$ is totally ramified at the prime $\lambda$ of $F_m$ above $\ell$, and $\lambda$ (being principal) splits completely in $F_m^{(1)}$, the extension $L'_m / F_m^{(1)}$ is ramified also at the $h$ primes of $F_m^{(1)}$ above $\ell$. In sum, this gives $\rho = 4 h$, and we find that the equality is satisfied whenever $h \geq 18$. Using that $h \rightarrow \infty$ as $m \rightarrow \infty$ (see [12]), we now get infinitely many $m$ such that $L'_m$ has an infinite class field tower. Note that $F_m^{(1)}$ and $L_m$ are linearly disjoint over $F_m$ since the former is unramified, and the latter is totally ramified at primes above $\ell$. By disjointness, $L'_m / L_m$ is abelian and unramified, and so $L_m$, and consequently $Q(\zeta_\ell)$, also have infinite class field towers. 

**Corollary 2.4.** Assume Conjecture 2.2. Then for each $k \in \{12, 16, 18, 20, 22, 26\}$, there are infinitely many primes $\ell$ such that $K_{\Delta_k, \ell}$ has an infinite class field tower.

**Proof.** It is easy to verify that primes $\ell$ of the form $m^2 + 3 m + 9$ are never congruent to $1$ mod $(k-1)$ for each $k$ in the list, so $(\ell-1, k-1) = 1$ for any $\ell$ constructed by the theorem. Avoiding the finitely many primes in the table given before Theorem 2.1 for which the representation is not surjective, the remaining primes constructed in Theorem 2.3 satisfy all of the hypotheses of Theorem 2.1. 

**Remark 2.5.** Hardy and Littlewood also provide an asymptotic version of their conjecture (see again [5]). Applied to the polynomial $h(k)$ used in the proof, the number $P_h(x)$ of primes less than $x$ which are represented by $h(k) = 144 k^2 + 84 k + 19$ satisfies

$$P_h(x) \sim \frac{1}{4} \prod_{p=5}^\infty \left( 1 - \frac{\frac{3888}{p}}{p-1} \right) \sqrt{x} \log x \approx \frac{28 \sqrt{x}}{\log x},$$

where we have used SAGE to approximate the constant by including the terms in the product for all primes $p \leq 10^7$. This thus also provides an asymptotic lower bound for the number of primes $\ell \leq x$ such that $Q(\zeta_\ell)$ has an infinite class field tower.
Finally, we remark that setting \( m = 12k + 2 \) in the proof of Theorem 2.1 was overly restrictive on our choice of \( m \), designed only to ensure that \( \ell \equiv 7 \mod 12 \). This can be equally well achieved by insisting that \( m \equiv 2, 7, 10, \) or \( 11 \mod 12 \). Searching Shanks' Table 1 for such values of \( m \) giving \( h \geq 18 \) provides the first few examples of \( \mathbb{Q} (\zeta_\ell) \) provided by the proof: \( \ell \in \{ 2659, 3547, 5119, 8563, \ldots \} \). Note that for each of these specific values of \( \ell \), Theorem 2.1 is proved unconditionally, the Hardy-Littlewood conjecture being used only to guarantee that there are infinitely many primes in this list.

3. **Infinite Class Field Towers from non-CM Elliptic Curves**

A second class of fields of arithmetic interest we discuss are the fixed fields of representations attached to elliptic curves. Let \( E \) be an elliptic curve without complex multiplication. Let \( \rho_n : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}/n) \) be the Galois representation associated to the \( n \)-torsion points of \( E \). Let \( A_E \) be the product of all the exceptional primes of \( E \), the finite set of primes \( \ell \) such that \( \rho_\ell \) is not surjective. Then for all \( n \) relatively prime to \( M_E := 30A_E \), the representation \( \rho_n \) is surjective, and hence \( \text{Gal}(K_n/\mathbb{Q}) \cong \text{GL}_2(\mathbb{Z}/n) \) (see [10, 9, 6]). We note that this set of primes, and hence the constants \( A_E \) and \( M_E \), have been studied extensively. In particular, we note that explicit bounds on these constants are known [1, Theorem A.1 and Theorem 2], and \( M_E = 30 \) for almost all elliptic curves (see Remark 3.3).

For a number field \( F \), let \( F^{(m)} \) denote the \( m \)-step in the Hilbert class field tower over \( F \).

**Theorem 3.1.** Let \( E/\mathbb{Q} \) be an elliptic curve without complex multiplication, and let \( \rho_n, K_n, A_E, \) and \( M_E \) be as in the preceding paragraph. Let \( S \) be the set of integers prime to \( M_E \). Then for all \( n \in S \) outside a subset of density zero, the field \( K_n \) has an infinite Hilbert class field tower. Furthermore, for such \( n \), there is a natural surjection of class groups \( \text{Cl}(K_n^{(m)}) \to \text{Cl}(\mathbb{Q}(\zeta_n)^{(m)}) \) for each \( m \geq 1 \).

**Proof.** For \( n \) prime to \( M_E \), the representation \( \rho_n \) is surjective, and so \( \text{Image}(\rho_n) \cong \text{Gal}(K_n/\mathbb{Q}) \cong \text{GL}_2(\mathbb{Z}/n) \). The fixed field of the kernel of the composite representation \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/n)^* \) arising from the exact sequence

\[
1 \to \text{SL}_2(\mathbb{Z}/n) \to \text{GL}_2(\mathbb{Z}/n) \to (\mathbb{Z}/n)^* \to 1
\]

is the \( n \)-th cyclotomic field \( \mathbb{Q}(\zeta_n) \), and so we have an inclusion of fields \( \mathbb{Q} \subset \mathbb{Q}(\zeta_n) \subset K_n \). By a result of Shparlinski (see [13]), the set of \( n \) coprime to \( M_E \) for which \( \mathbb{Q}(\zeta_n) \) has an infinite class field tower has density one in the set of integers coprime to \( M_E \). For the remainder of the proof, \( n \) will denote such an integer. We claim that the fields \( \mathbb{Q}(\zeta_n)^{(m)} \) and \( K_n \) are linearly disjoint extensions of \( \mathbb{Q}(\zeta_n) \) for all \( m \geq 1 \). Let \( H_{n,m} \) denote their intersection. Consider the lattice diagram of fields:

\[
\begin{tikzcd}
\mathbb{Q}(\zeta_n)^{(m)} \arrow{dr} \arrow{ur} & K_n \\
H_{n,m} \\
\mathbb{Q}(\zeta_n)
\end{tikzcd}
\]

Since \( \mathbb{Q}(\zeta_n)^{(m)}/\mathbb{Q}(\zeta_n) \) is a Galois extension with solvable Galois group (being constructed via a series of abelian extensions), so is \( H_{n,m}/\mathbb{Q}(\zeta_n) \). But \( \text{Gal}(K_n/\mathbb{Q}) \cong \text{Gal}(\mathbb{Q}(\zeta_n)^{(m)}/\mathbb{Q}(\zeta_n)) \cong (\mathbb{Z}/n)^* \) is surjective. This shows that \( \text{Gal}(H_{n,m}/\mathbb{Q}(\zeta_n)) \) is also surjective, so \( \text{Gal}(H_{n,m}/\mathbb{Q}(\zeta_n)) \cong (\mathbb{Z}/n)^* \cong (\mathbb{Z}/n)^* \).
By the above techniques, \( K_n \) is unramified outside \( n \) and thus \( K_n \) is contained in the maximal such extension \( K^{(m)}_{n,m} \). The restriction map on Galois groups

\[
\text{Gal}(K^{(m+1)}_n/K^{(m)}_n) \longrightarrow \text{Gal}(K^{(m)}_n \mathbb{Q}((\zeta_n)^{(m)}/K^{(m)}_n) \cong \text{Gal}(\mathbb{Q}(\zeta_n)^{(m+1)}/\mathbb{Q}(\zeta_n)^{(m)})
\]

corresponds by class field theory to the desired surjection \( \text{Cl}(K^{(m)}_n) \to \text{Cl}(\mathbb{Q}(\zeta_n)^{(m)}) \) of class groups.

**Remark 3.2.** The density result of Shparlinski used in the proof is based on an explicit construction due to Furuta (see [4, Theorem 4]). Namely, we can find explicit examples of the \( n \) described in the theorem by choosing a rational prime \( \ell \) and taking \( n \) to be a product of nine or more rational primes congruent to 1 mod \( \ell \) and prime to \( M_E \). The field \( K_n \) then has an infinite \( \ell \)-class field tower. For example, consider the elliptic curve

\[ E : y^2 + y = x^3 - x \]

of conductor 37. By [10, 5.5.6, Page 310] we find that \( A_E = 1 \) and so \( M_E = 30 \). We take \( n \) to be the product of the first nine primes which are congruent to 1 mod 5:

\[ n = 11 \cdot 31 \cdot 41 \cdot 61 \cdot 71 \cdot 101 \cdot 131 \cdot 151 \cdot 181. \]

Then \( K_n \) has an infinite Hilbert 5-class field tower and is unramified outside primes dividing 37n.

**Remark 3.3.** The constant \( A_E \) in Serre’s Theorem has been studied extensively. In [3] it was shown that almost all elliptic curves over \( \mathbb{Q} \) have Serre constant \( A_E = 1 \) (and thus \( M_E = 30 \)). Thus for almost all elliptic curves over \( \mathbb{Q} \) and almost all integers \( n \) with \( (n, 30) = 1 \), the field \( K_n \) has an infinite class field tower.

Finally, we note that variants of these techniques apply to other arithmetically significant fields. For example, let \( E \) be a semistable elliptic curve over \( \mathbb{Q} \) of prime conductor \( \ell \geq 11 \), and suppose that \( \mathbb{Q}((\zeta)) \) has an infinite Hilbert class field tower. By the above techniques, \( K_{E,\ell} \) has an infinite Hilbert class field tower. Further, \( K_{E,\ell} \) is unramified outside \( \ell \), and by a well-known theorem of Mazur (see [7]), we have \( \text{Gal}(K_{E,\ell}/\mathbb{Q}) = \text{GL}_2(\mathbb{Z}/\ell) \). Unfortunately, it is unknown if there exists an elliptic
curve of conductor $\ell$ for infinitely many primes $\ell$ (though this is widely believed). Regardless, an examination of Cremona’s tables of elliptic curves (see [2]) shows that there are no elliptic curves with conductor 877 but that there exist elliptic curves with conductor 3547, the second prime provided in the discussion after Corollary 2.4. Thus we can find examples of elliptic curves to which this variant approach applies.

References

1. Cojocaru, Alina Carmen. On the surjectivity of Galois representations associated to non-CM elliptic curves. Canad. Math. Bull., 48(1):16–31, 2005.
2. John Cremona, Algorithms for modular elliptic curves online edition.
3. W. D. Duke, Elliptic curves with no exceptional primes, C. R. Math. Acad. Sci. Paris Ser. I 325 (1997), pp. 813-818.
4. Yoshimori Furuta. On Class Field Towers and the Rank of Ideal Class Groups. Nagoya Math J, 48, 1972. 147-157.
5. G.H. Hardy and J. E. Littlewood. Some problems of ‘Partitio numerorum’; III: On the expression of a number as a sum of primes. Acta Math. 44 (1923), no. 1, 1–70.
6. Kani, Ernst. Appendix to: On the surjectivity of Galois representations associated to non-CM elliptic curves. Canad. Math. Bull., 48(1):16–31, 2005.
7. Barry Mazur. Rational Isogenies of prime degree, Invent. Math. 44 (1978), pp. 129–162.
8. Rene Schoof, Infinite class field towers of quadratic fields, J. Reine Angew. Math. 372 (1986), 209–220.
9. Jean-Pierre Serre, Abelian $\ell$-adic representations and elliptic curves, McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute, W. A. Benjamin, Inc., New York-Amsterdam, 1968.
10. —, Propriétés Galoisienes des points d’ordre fini des courbes elliptiques, Inventiones Mathematicae 15, 1972, pp. 259-331.
11. —, Congruences et formes modulaires [d’après H. P. F. Swinnerton-Dyer], Séminaire Bourbaki 24e année (1971/1972), Exp. No. 416, Springer, Berlin, 1973, pp. 319338. Lecture Notes in Math., Vol. 317.
12. Daniel Shanks. The Simplest Cubic Fields. Mathematics of Computation, Volume 28, Number 128. 1974. 1137-1152.
13. Igor E. Shparlinski, Infinite Hilbert class field towers over cyclotomic fields, Glasg. Math. J. 50 (2008), no. 1, 2732.

Math. department, University of Arizona, 617 N Santa Rita, Tucson, AZ. 85721-0089, USA.
E-mail address: kirti@math.arizona.edu

Math. department, Willamette University, 800 State Street, Salem, OR. 07304-0089, USA.
E-mail address: cmcleman@willamette.edu