Introduction

The aim of this paper is to show some equidistribution statements of Galois orbits of CM-points for quaternion Shimura varieties. These equidistribution statements will imply the Zariski densities of CM-points as predicted by André-Oort conjecture (see §1). Our main result (Corollary 2.6) says that the Galois orbits of CM-points with the maximal Mumford-Tate groups are
equidistributed provided some subconvexity bounds on Rankin-Selberg $L$-series and on torsions of the class groups. A proof of the subconvexity bound for $L$-series has been announced by Michel and Venkatesh.

Combining with some work of Cogdell, Michel, Piatetski-Shapiro, Sarnak, and Venkatesh, we obtain the following unconditional results about the equidistribution of CM-points in the following cases:

1. **Full CM-orbits on quaternion Shimura varieties** (Theorem 2.1). This is a generalization of work of Duke [12] for modular curves, Michel [21], and Harcos-Michel [17] for Shimura curves over $\mathbb{Q}$.

2. **Galois orbits of CM-points with a fixed maximal Hodge-Tate group** (Corollary 2.7). Under our setting, this strengthens a result of Edixhoven and Yafaev [16] about the finiteness of CM-points on a curve with fixed $\mathbb{Q}$-Hodge structure.

The maximality condition of the Hodge-Tate group automatically holds in dimension one case (proposition 6.2), and can be classified in dimension 2 case (Proposition 6.3). In higher dimension case, we will give many examples of Shimura varieties where maximality condition holds (Proposition 6.4-6.8).

The proofs of these results have two parts. In the first part (§3-4), we will give an estimate on probability measures on CM-suborbits (Theorem 2.2) which follows from the central value formulas proved in our previous paper and Waldspurger’s paper, the study of Hecke orbits of CM-points, and analysis of the spectral decomposition. In the second part (§5-6), we will study the Mumford-Tate group of CM-points and estimate the size of Galois orbits in terms of discriminants of the torsion in class groups.

**Acknowledgement.** I would like to thank Bas Edixhoven, Dihua Jiang, Jian-Shu Li, Philippe Michel, Frans Oort, Peter Sarnak, Emmanuel Ullmo, and Akshay Venkatesh for many helpful discussions. This work has been supported by Chinese Academy of Sciences, Tsinghua University, and National Science Foundation. I also want to thank the referee for bring my attention to Waldspurger’s paper.

## 1 Conjectures

In this section we will introduce the André-Oort conjecture and the equidistribution conjecture. For background on Shimura varieties, we refer to Deligne
For the André-Oort conjecture, we refer to Moonen [22] and Edixhoven [13]. Notice that questions about the equidistribution of CM-points have previously been addressed in Clozel-Ullmo [4]. See also Noot [25] for a detailed survey of recent progress.

Let $M$ be a connected Shimura variety defined over a number field $E$ in $\mathbb{C}$. Then for any Shimura subvariety $Z$, the set of CM-points on $Z$ is Zariski dense. The conjecture of André-Oort says that the converse is true:

**Andre-Oort conjecture ([1, 26, 22, 13]).** Let $Z$ be a connected subvariety of $M$ which contains a Zariski dense subset of CM-points. Then $Z$ is a Shimura subvariety.

Let’s recall the description of Shimura subvarieties. Assume that $M$ is a connected component of a Shimura variety $M_U$ of the form

$$M_U(\mathbb{C}) = G(\mathbb{Q}) \backslash X \times G(\mathbb{\hat{Q}})/U, \quad M = \Gamma \backslash X$$

where

- $G$ is an algebraic group over $\mathbb{Q}$ of adjoint type,
- $X$ is a $G(\mathbb{R})$-conjugacy class of embeddings
  $$h : S := \text{Res}_{\mathbb{C}/\mathbb{R}} G_{m} \longrightarrow G_{\mathbb{R}}$$
  of algebraic groups over $\mathbb{R}$,
- $U$ is an open and compact subgroup of $G(\mathbb{\hat{Q}})$, $\Gamma = G(\mathbb{Q}) \cap U$.

For each point $x \in M_U(\mathbb{C})$, the minimal (connected) Shimura subvariety containing $x$ can be defined as follows. Let $(h, g) \in X \times G(\mathbb{\hat{Q}})$ represent $x$. Let $H$ denote the Zariski closure of $h(U(\mathbb{C}))$ in $G$ as an algebraic subgroup over $\mathbb{Q}$ which is called the Mumford-Tate group of $x$. The Hodge closure $M_{U,x}$ of $x$ in $M_U$ is defined to be the subvariety of $M$ represented by $H(\mathbb{R}) \times X \times H(\mathbb{\hat{Q}}) g$. The minimal Shimura subvariety is the connected component of $M_{U,x}$ containing $x$ which has the form

$$M_x := \Gamma' \backslash X', \quad \Gamma' := H(\mathbb{Q}) \cap gUg^{-1}, \quad X' := H(\mathbb{R})h.$$

A point $x \in M_U(\mathbb{C})$ is a CM-point if and only if $M_x$ is 0-dimensional, or equivalently, $H$ is a torus.
Remarks.

1. This conjecture remains open, although many special cases have been treated by Moonen [22, 23, 24], Edixhoven [13, 14, 15], Edixhoven-Yafaev [16], and Yafaev [32, 33]. In particular, the conjecture is true when $Z$ is a curve under one of the following assumptions:

- $M$ is a product of two modular curves (Andre [2]);
- CM-points on $Z$ are in a single Hecke orbit (Edixhoven-Yafaev [16]);
- GRH for CM fields (Yafaev [33]).

2. This conjecture is analogous to the Manin-Mumford conjecture proved by Raynaud [27] about torsion points in abelian variety. The Manin-Mumford conjecture is also a consequence of the equidistribution conjecture proved using Arakelov theory (Ullmo-Szpiro-Zhang [28], Ullmo [29], Zhang [34]).

In this paper we want study the distribution property of CM-points. We want to propose the following conjecture about distributions of CM-points:

**Equidistribution Conjecture.** Let $x_n$ be a sequence of CM-points on $M$. Assume that for any proper Shimura subvariety $Z$, there are only finitely many points in $x_n$ contained in $Z$. Then the Galois orbit $O(x_n)$ of $x_n$ is equidistributed with respect to the canonical measure on $M$.

Here the canonical measure $d\mu$ means the probability measure induced from the invariant measure on the Hermitian symmetric domain $X$ in the definition of Shimura variety. Equidistribution means that for any continuous function $f$ on $M(\mathbb{C})$ with compact support, we have the limit:

$$\frac{1}{\#O(x_n)} \sum_{y \in O(x_n)} f(y) \longrightarrow \int_{M(\mathbb{C})} f(x) d\mu(x).$$

Remarks

1. To see how the equidistribution conjecture implies the Andre-Oort conjecture, we first assume that $M$ does not have a proper Shimura subvariety containing $Z$. Then we may list all Shimura subvarieties of $M$ in a sequence $M_1, M_2, \cdots, M_n, \cdots$. Now by induction, for each $n$, we may find a CM-point $x_n$ on $Z$ which is not in the union of the first $n$ $M_i$'s. In this way, $\{x_n\}$ becomes a strict sequence of CM-points in $M$. The equidistribution
conjecture implies that the Galois orbits of the $x_n$ are equidistributed. Since all these Galois orbits are included in $Z(\mathbb{C})$, we must have $Z = M$.

2. In the simplest case where $M$ is the modular curve $X_0(1)$, the conjecture is a theorem of Duke [12]. In the case where $M$ is defined by an algebraic group with positive $\mathbb{Q}$-rank, the equidistribution of Hecke orbits has been proved by Clozel-Ullmo [4] and Clozel-Oh-Ullmo [7].

3. The equidistribution conjecture also implies (and is implied by) the equidistribution of Shimura subvarieties in $M$. When these subvarieties are defined by semisimple-subgroups not included in any proper parabolic subgroup, the equidistribution has been proved by Clozel and Ullmo [5] by ergodic method. In [19], Jiang, Li and the author proved an explicit period integral formula for cycles in the middle dimension, and was able to deduce the equidistribution with precise rate of convergence of probability measures.

2 Statements

In this section, we state our main results on the equidistribution of Galois orbits of CM-points on quaternion Shimura varieties. Let us start with some definitions and notations.

**Quaternion Shimura varieties.** Let $F$ be a totally real number field of degree $g$, and let $B$ be a quaternion algebra over $F$. Then for each real embedding $\sigma$ of $F$, $B \otimes_\sigma \mathbb{R}$ is either isomorphic the matrix algebra $M_2(\mathbb{R})$ or the Hamilton quaternion algebra $\mathbb{H}$. Let $G$ denote the algebraic group $B^\times / F^\times$ over $\mathbb{Q}$. Then

$$G(\mathbb{R}) = \prod_\sigma (B \otimes_\sigma \mathbb{R})^\times / \mathbb{R}^\times \simeq \text{PGL}_2(\mathbb{R})^d \times \text{SO}_{3g-3}$$

where $\sigma$ runs though the set of real embeddings of $F$. Via such an isomorphism $G(\mathbb{R})$ acts on

$$X := (\mathbb{C} \setminus \mathbb{R})^d = (\mathbb{H}^\pm)^d.$$  

In terms of Shimura datum, $X$ can be considered as the $G(\mathbb{R})$-conjugacy class of the embedding:

$$h_0 : \mathbb{S} \to G_{\mathbb{R}}$$

which sends $a + bi \in \mathbb{S}(\mathbb{R}) = \mathbb{C}^\times$ to an element whose components are represented by $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ in $\text{PGL}_2(\mathbb{R})$ and by 1 in $\text{SO}_3(\mathbb{R})$. 

5
For any abelian group $A$ let $\hat{A}$ denote $A \otimes \varprojlim \mathbb{Z}/n\mathbb{Z}$. Then for any open and compact subgroup $U$ of $G(\hat{\mathbb{Q}})$ we have an analytic variety

$$M_U(C) := G(\mathbb{Q}) \setminus X \times G(\hat{\mathbb{Q}})/U.$$ 

If $d > 0$, by Shimura’s theory, the variety $M_U$ is defined over the following totally real subfield:

$$\widetilde{F} = \mathbb{Q} \left( \sum_{\sigma \in S} \sigma(x), \quad \forall x \in F \right)$$

where $S$ denotes the real embeddings $\sigma$ such that $B \otimes_{\sigma} \mathbb{R} \simeq M_2(\mathbb{R})$. The action of the Galois group $\text{Gal}(\overline{\mathbb{Q}}/\widetilde{F})$ on the connected components is given by a reciprocity homomorphism:

$$\text{Gal}(\overline{\mathbb{Q}}/\widetilde{F}) \longrightarrow F^+_{x} \setminus \hat{F}/\nu(U).$$

In the following we will fix a maximal order $\mathcal{O}_B$ of $B$ and will take $U$ to be the subgroup $\hat{\mathcal{O}}_{B} \otimes \mathcal{O}_{\hat{F}}$ of $G(\hat{\mathbb{Q}})$. Let $N$ denote the level of $M$, which is by definition the product of prime ideals $\wp$ over which $B$ does not split. Up to isomorphisms, both $B$ and $M_U$ are determined by the pair $(S, N)$.

**CM points.** A point $x$ in $M_U(C)$ is a CM point if and only if it is represented by a pair $(h, g) \in X \times G(\hat{\mathbb{Q}})$ such that the stabilizer of $x$ in $G(\mathbb{Q})$ is a torus $T := K^\times /F^\times$, where $K$ is a quadratic CM-extension of $F$ embedded into $B$. Here are some invariants of CM-points:

1. the order

$$\mathcal{O}_x := K \cap g \mathcal{O}_{B} g^{-1} = \mathcal{O}_F + c(x) \mathcal{O}_K,$$

where $c(x)$ is an ideal of $\mathcal{O}_F$ called the conductor of $x$.

2. the type $(K, S_K)$, where $S_K$ is the set of the complex embeddings of $K$ so that the action of a $t \in K^\times$ on the tangent space of $X$ at $h$ has eigenvalues given by

$$\sigma(t/\bar{t}), \quad \sigma \in S_K.$$ 

When $d > 0$, $x$ is defined over an abelian extension of a CM-subfield of $\mathbb{C}$ which is given by:

$$\overline{K} = \mathbb{Q} \left( \sum_{\sigma \in S_K} \sigma(t), \quad \forall t \in K \right).$$
More precisely, there is a homomorphism

\[ r_x : \text{Gal}(\bar{\mathbb{Q}}/\bar{K}) \to T(\mathbb{Q}) \setminus T(\hat{\mathbb{Q}})/O_x \]

such that for \( \gamma \in \text{Gal}(\bar{\mathbb{Q}}/\bar{K}) \), the conjugate \( \gamma x \) is a CM-point represented by \( (h, r(\gamma)g) \). Let \( O_{cm}(x) \) denote the CM-orbit of \( x \) consisting of points represented by \( (h, t) \) with \( t \in T(\hat{\mathbb{Q}}) \), and let \( O_{gl}(x) \) denote the Galois orbit of \( x \) under \( \text{Gal}(\bar{\mathbb{Q}}/\bar{K}) \). Then, \( O_{gl}(x) \subset O_{cm}(x) \). When \( d = 1 \), we have \( O_{gl}(x) = O_{cm}(x) \). In general, they are different. In fact, the Galois orbit is included in the Hodge orbit \( O_{hg}(x) \) defined to be the set of points represented by \( (h, t) \) with \( t \in H(\hat{\mathbb{Q}}) \), where \( H \subset T \) is the Mumford-Tate subgroup of \( x \).

By a CM-suborbit \( O(x) \) of a CM-point, we mean an orbit \( O(x) \subset O_{cm}(x) \) under an open subgroup of \( T(\mathbb{Q}) \setminus T(\hat{\mathbb{Q}}) \). Its conductor \( c(O(x)) \) is defined to be the largest ideal \( c \) so that \( (1 + \hat{c}\mathcal{O}_K) \times \) stabilizes \( O(x) \).

The equidistribution conjecture implies the equidistribution of \( O_{cm}(x) \):

**Theorem 2.1.** Let \( x_i \) be a sequence of CM-points on \( M_U \). Then the CM-points \( O_{cm}(x_i) \) are equidistributed.

This is a direct generalization of Duke’s result [12]. The proof of this theorem uses some bounds on Hecke eigenvalues by Kim-Shahidi for \( \text{GL}_2 \)-forms and on the central value of the \( L \)-series \( L(1/2, f \otimes \epsilon_{K/F}) \) by Cogdell-Piatetski-Shapiro-Sarnak for holomorphic \( f \), and by Venkatesh [30] for general \( f \), where \( \epsilon_{K/F} \) is the quadratic character of \( \hat{F} \times \) associated to the extension \( K/F \). In the following, we want to extend this result to certain sub-orbits of \( O_{cm}(x) \) under the following assumption:

**\( \delta \)-bound.** Let \( \delta \) be a positive number. There are constants \( C \) and \( A \) such that for any eigenform \( f \in C^\infty(X(\mathbb{C})) \) the following two conditions are verified:

1. The local parameters \( \alpha_v \) of \( L(s, f) \) are bounded as follows:

\[ |\alpha_v| \leq C\lambda(f)^A q_v^{\delta} \]

where \( \lambda(f) \) is the eigenvalue of \( f \) under the Laplacian operator on \( M_U \), and \( q_v \) is the cardinality of the residue field of \( \mathcal{O}_F \).

2. For any imaginary quadratic extension \( K \) of \( F \) with absolute discriminant \( \text{disc}(K) \), and any finite character \( \chi \) of the group \( K^\times \setminus \hat{K}^\times /\hat{F}^\times \):

\[ |L(1/2, \chi, f)| \leq C\lambda(f)^A \text{disc}(\chi)^{\delta}, \]

7
where $L(s, f, \chi)$ is the Rankin-Selberg convolution of $L_F(s, f)$ and $L_K(s, \chi)$, and $\text{disc}(\chi)$ denotes $N_{F/Q}(c(\chi)^2\text{disc}_F(K))$.

**Remarks**

1. The $\delta$-bounds assumption always hold for $\delta = 1/2 + \epsilon$, which is called a convexity bound; any bound with $\delta < 1/2$ is called a subconvexity bound.

2. For the first inequality, the Peterson-Ramanujan conjecture says that the absolute value of $\alpha_v$ is always 1. So $\delta$ could be any positive number. The recent work of Kim-Shahidi [20] implies that the inequality hold for $\delta = 1/9 + \epsilon$.

3. By GRH, we should have second inequality for any $\delta > 0$. When $F = Q$, the subconvexity has been proven by Michel [21] for holomorphic forms $f$ with $\delta = 1/2 - 1/1145$, and by Harcos-Michel [17] for Mass forms $f$ with $\delta = 1/2 - 1/2491$. For general $F$ and quadratic $\chi$, the subconvexity has been proven by Cogdell-Piatetski-Shapiro-Sarnak [9, 8] for holomorphic forms with $\delta = 1/2 - 7/130$ and for non-holomorphic forms by Venkatesh [30].

4. The work of Venkatesh actually holds for any family of $L$-series of a fixed $GL_2$-form twisted by central characters over any number field. In particular, when $f$ and $K$ are fixed, the subconvexity bound for $L$-series holds. Indeed, let $g$ be the base change of $f$ over $GL_2(K)$. Then

$$L_F(s, \chi, f) = L_K(s, g \otimes \chi).$$

**Theorem 2.2.** Let $\delta$ be a positive number such that the $\delta$-bounds hold. Let $f$ be a function on $M_{U}(\mathbb{C})$ which has integral 0 on each connected component and which is constant outside of a compact subset. Then for any $\epsilon > 0$, there is a constant $C(f, \epsilon)$ such that

$$\left| \sum_{y \in O(x)} f(x) \right| \leq C(f, \epsilon)\text{disc}(x)^{1/4 + \delta/2 + \epsilon}$$

for any CM-suborbits $O(x)$.

**Remarks**

1. The equality is non-trivial only if $O(x)$ has size bigger than $\text{disc}(x)^{\delta/2 + 1/4}$.

2. For the proof we only need $\delta$ to satisfy the $\delta$-assumption for $\chi$ trivial on $O(x)$.
Corollary 2.3. Let $\delta$ be a positive number such that the $\delta$-bounds hold. Let $O(x_n)$ be a sequence of CM-suborbits in a connected component $M$ of $M_U$ satisfying the equality

$$\#O(x_n) \geq \text{disc}(x_n)^{\delta/2+1/4+\epsilon}$$

for some fixed $\epsilon > 0$. Then the $O(x_n)$ are equidistributed on $M(\mathbb{C})$.

Remarks

1. Theorem 2.1 follows from Corollary 2.3, since we have the Brauer-Siegel theorem:

$$\lim_{n \to \infty} \frac{\log \#O_{\text{cm}}x_n}{\log \text{disc}x_n} = \frac{1}{2}.$$ 

2. If we assume the Riemann-Hypothesis, then we take $\delta = 0$ in the second assumption to get the exponent $1/4 + \epsilon$. This is essentially optimal. To give an example, we assume that $F$ is a real quadratic field, $B = M_2(F)$, that $x_n$ are in a single modular curve $C$, and that $O(x_n)$ is the full CM-orbits on $C$. Since the discriminant of $x_n$ on $M$ is the square of that on $C$, then the Brauer-Siegel theorem gives

$$\lim_{n \to \infty} \frac{\log \#O_{\text{cm}}x_n}{\log \#O(x_n)} = \frac{1}{4}.$$ 

Equidistribution of Galois orbits

In the following we want to give some examples of CM-points whose Galois orbits are equidistributed by Corollary 2.3.

Recall that $S$ is the set of all real embeddings of $F$ over which $B$ is split. Let $F_0$ the subfield of $F$ on which the restrictions of all embeddings in $S$ give the same embeddings. Let $\bar{F}$ be a Galois closure of $F$ over $F_0$.

Theorem 2.4. Assume that $d = 2$ and that $[\bar{F} : F_0]$ is a power of 2. Then the subconvexity bound implies the equidistribution of Galois orbits of CM-points $x$ with the equality $K_0(x) = F_0$. Here, when $x$ has CM-type $(K, \lbrace \sigma_1, \sigma_2 \rbrace)$, $K_0(x)$ denotes the subfield of $K$ of elements satisfying $\sigma_1(x) = \sigma_2(\bar{x})$.

Remarks.

1. If we only consider CM-points with fixed CM-field $K$, then the condition on $[F : F_0]$ can be dropped.
2. For Hilbert modular surfaces, the subconvexity bound implies the equidistribution of Galois orbits of CM-points which are not included in any Shimura curves.

The idea of the proof of this proposition is to show that for a CM-point $x$ with CM field $K$, the reciprocity map

$$r_x : \text{Gal}(\overline{\mathbb{Q}}/\overline{K}) \longrightarrow T(\mathbb{Q})/T(\overline{\mathbb{Q}}) = \text{Pic}(\mathcal{O}_x)/\text{Pic}(\mathcal{O}_F)$$

has cokernel annihilated by some positive integer $n$ depending on the Mumford-Tate group. We may drop the assumption that $[\overline{F} : F_0]$ is a power of 2 under the following assumption:

**$\epsilon$-conjecture.** Fix a totally real number field $F$, a positive integer $n$, and a positive number $\epsilon$. Then, for any quadratic CM-extension $K$, and any order $\mathcal{O}$ of $K$ containing $\mathcal{O}_F$, the $n$-torsion of the class group of $\mathcal{O}_c$ has the following bound:

$$\#\text{Pic}(\mathcal{O}_c)[n] \leq C(\epsilon)\text{disc}(\mathcal{O}_c)^{\epsilon},$$

where $C(\epsilon)$ is a positive constant depending only on $\epsilon$.

**Remarks**

1. We will reduce to the case where $\mathcal{O}_c = \mathcal{O}_K$ is maximal and $n$ is an odd (Corollary 5.4).
2. By the Brauer-Siegel theorem, $1/2 + \epsilon$ will be the trivial bound.
3. When $n = 2$, $K = \mathbb{Q}\sqrt{D}$, with $D \in \mathbb{Z}$ a fundamental discriminant, and the conjecture is true by Gauss’ genus theory. Actually, the 2-torsion of a class group equals $2^\delta$ where $\delta$ is the number of prime factors of $D$. We will prove the conjecture for 2-torsion for an arbitrary CM-extension (Corollary 5.4).
4. When $n = 3$, Helfgott and Venkatesh obtain the bound $\epsilon = 0.44187$.
5. In Brumer-Silverman [3], the following stronger bound has been formulated:

$$\log \#\text{Cl}(L)[n] \leq C \log \text{disc}(L)/\log \log \text{disc}(L).$$

**Theorem 2.5.** Assume the $\epsilon$-conjecture (for a positive integer $n$ as specified in Corollary 5.2). Then we have the following estimate for the size of Galois orbits for a CM-point $x$ on $M_U$ with maximal Mumford-Tate group $H = T$:

$$\#O_{\text{gl}}(x) >> \text{disc}(x)^{1/2-\epsilon}.$$

Applying Corollary 2.3, we obtain:
Corollary 2.6. The $\epsilon$-conjecture and subconvexity bound imply the equidistribution of CM-points with maximal Mumford-Tate group $H = T$.

Corollary 2.7. The equidistribution holds for Galois CM-points with a fixed maximal Mumford-Tate group $H = T$. In particular any infinite set of such CM-points are Zariski dense.

Remarks.

1. In our current setting, the Zariski density in Corollary 2.7 strengthens a theorem of Edixhoven-Yafaev [16] about the finiteness of CM-points with fixed Hodge $\mathbb{Q}$-structure on a non-Hodge curve. Our finiteness holds for any proper subvariety. Of course, their theorem applies to general Shimura varieties.

2. Theorem 2.4 follows from this Corollary and Proposition 6.3, which says that $H$ is the kernel of the norm

$$N_{K/K_0} : K^\times/F^\times \longrightarrow K_0^\times/F_0^\times.$$

3. When $d > 2$, we don’t have a general description of CM-points having maximal Mumford-Tate orbits, except for some partial results given in §6. In particular, we can show that $H = T$ for all CM-points if $d$ is odd and if $F/F_0$ is abelian with Galois group verifying one of the following two conditions are verified:

- $[F : F_0]$ is a power of 2 (Corollary 6.6), or
- $\text{Gal}(F/F_0)$ has cyclic 2-Sylow subgroup and $d < p$ for any odd prime factor of $[F : F_0]$ (Corollary 6.8).

Thus we have equidistribution of Galois orbits of all CM points on these Shimura varieties.

3 Hecke orbits

In this section and the next, we want to prove Theorem 2.2. More precisely, we want to estimate the sum:

$$\ell(f; O(x)) := \sum_{y \in O(x)} f(x)$$
for a CM-suborbit $O(x)$ and for a function $f$ on $M_U(\mathbb{C})$ which has integral 0 on each connected component and is constant outside of a compact set. In this section we want to reduce the computation of this integral to the case where $x$ and $O(x)$ have the same conductor. (See Proposition 3.4.)

Let $\Gamma$ be the stabilizer of $O(x)$ in $T(\mathbb{Q})\backslash T(\hat{\mathbb{Q}})$ with index $i(\Gamma)$. Then we have

$$\ell(f, O(x)) = i(\Gamma)^{-1} \sum_{\chi} \ell_{\chi}(f; x)$$

where $\chi$ run through characters of $T(\mathbb{Q})\backslash T(\hat{\mathbb{Q}})/\Gamma$, and

$$\ell_{\chi}(f; x) := \sum_{t \in T(\mathbb{Q})\backslash T(\hat{\mathbb{Q}})/\hat{O}_x} \chi^{-1}(t)f(tx).$$

Let $K$ be the CM field defining $x$. Then the set of CM-points with field $K$ is given by

$$T(\mathbb{Q})\backslash G(\hat{\mathbb{Q}})/U = K^\times \backslash \hat{B}^\times / \hat{F}^\times \hat{O}_B^\times.$$

For each ideal $c$, the CM-points of conductor $c$ are represented by $g \in \hat{B}^\times$ such that

$$g\hat{O}_B g^{-1} \cap K = \mathcal{O}_c.$$

The set of CM-points with conductor $c$ is a single orbit under left multiplication by $\hat{K}^\times$. Thus the value $\ell_{\chi}(f, x)$ depends only on the conductor of $x$ up to multiple by a root of unity.

Let’s define a distinguished CM-point $x_c$ which is represented by $g_c$ with components $g_v \in B_v^\times$ given as follows. If $v$ does not divide $c$, we take $g_v = 1$. For $v$ dividing $c$, we have an isomorphism $B_v \simeq M_2(F_v)$ so that $\mathcal{O}_{K,v}$ is embedded into $M_2(\mathcal{O}_v)$. The action of $K_v$ on $F_v^2$ identifies $F_v^2$ with $K_v$ as a $K_v$-modules. The map $\alpha \rightarrow \alpha(\mathcal{O}_{K,v})$ defines a bijection between the set of $B_v^\times / \mathcal{O}_{B,v}^\times$ and the set of $\mathcal{O}_v$-lattices of $K_v$. The conductor of $\alpha$ is exactly the conductor of the $\mathcal{O}_v$-endomorphism algebra of the lattices. Thus we may take $g_v$ such that $g_v(\mathcal{O}_{K,v}) = \mathcal{O}_{c,v}$.

Now fix an anticyclotomic character $\chi$ of conductor $c = c(\chi)$. For each ideal $n$, we define a function $\gamma_n$ on CM-points with field $K$ supported on set of CM-points of conductor $nc$ and such that

$$\gamma_n(tx_{nc}) = \chi(t), \quad \forall t \in T(\hat{\mathbb{Q}}).$$
Let $r_{\chi}(m)$ be a function on nonzero ideals of $\mathcal{O}_F$ defined by the formula

$$r_{\chi}(m) = \begin{cases} \sum_{N(n)=m} \chi(n) & \text{if } (m, c) = 1 \\ 0 & \text{if } (m, c) \neq 1. \end{cases}$$

**Proposition 3.1.** For $m$ an ideal prime to $N$,

$$T_m \gamma_1 = \sum_n r_{\chi}(m/n) \gamma_n.$$

**Proof.** It is clear that $T_m \gamma_1$ still has character $\chi$ under left multiplication by $T(\bar{Q})$. Thus we have a decomposition:

$$T_m \gamma_1 = \sum a_{m,n} \gamma_n.$$

The number $a_{m,n}$ can be expressed as follows:

$$a_{m,n} = T_m \gamma_1(\mathcal{O}_{nc}) = \sum_{\Lambda} \gamma_1(\Lambda).$$

Here the sum is over sublattices of $\widetilde{\mathcal{O}}_{nc} := \prod_{v|mnc} \mathcal{O}_{nc,v}$ of index $m$. Notice that $\gamma_1(\Lambda) \neq 0$ if and only if $\Lambda$ has the form $t\mathcal{O}_c$ for some $t \in \bar{K}$. In this case $\gamma_1(\Lambda) = \chi(t)$. The condition that $\Lambda \subset \mathcal{O}_{nc}$ with index $m$ is equivalent to $m\mathcal{O}_{nc} \subset \Lambda = t\mathcal{O}_c$ with index $m$, which is equivalent to $mt^{-1}\mathcal{O}_{nc} \subset \mathcal{O}_c$ with index $m$. This last condition is equivalent to

$$mt^{-1} \in \mathcal{O}_c, \quad N_F(mt^{-1})n = m.$$ 

The second condition is $N_F(t) = mn$. Thus $t^{-1} = \bar{t}(mn)^{-1}$ and the first equation becomes $t \in n\mathcal{O}_c$. Write $t = ns$, then $N(s) = m/n$, and $\chi(t) = \chi(s)$. Thus we obtain

$$a_{m,n} = \sum_s \chi(s)$$

where $s$ runs through elements in $\mathcal{O}_c/\mathcal{O}_c^\times$ with norm $m/n$.

If $m/n$ is not prime to $c$, there is a prime $\pi$ dividing both $c$ and $s$. For each $s$ in the sum above, we may write $s = \pi tu$, where $t$ runs through representatives of $\mathcal{O}_{c/\pi}/\mathcal{O}_{c/\pi}^\times$ and $u$ runs through $\mathcal{O}_{c/\pi}^\times/\mathcal{O}_c^\times$. Thus we have

$$a_{m,n} = \chi(\pi) \sum \chi(t) \sum \chi(u).$$

As $\chi$ has conductor $c$, the sum of $\chi(u)$ is certainly $0$. \qed
Write
\[ L(s, \chi) = \sum_n \frac{\chi(n)}{N(n)^s}. \]
By the proposition, we have formally,
\[ \sum_m \frac{T_m \gamma_1}{Nm^s} = L(s, \chi) \cdot \sum_n \frac{\gamma_n}{Nn^s}. \]
It follows that
\[ \sum_n \frac{\gamma_n}{Nn^s} = L(s, \chi)^{-1} \sum_m \frac{T_m \gamma_1}{Nm^s}. \]
In other words,
**Corollary 3.2.**
\[ \gamma_n = \sum_{m | n} s_\chi(n/m) T_m \gamma_1 \]
where \( s_\chi(n) \) are coefficients of \( L_K(s, \chi)^{-1} \):
\[ s_\chi(n) = \sum_{N_K/F(a) = n} \chi(a) \cdot \mu(a) \]
where \( \mu(a) \) is the Möbius function on the ideals of \( \mathcal{O}_K \).

We may express \( \ell_\chi(f; x_{nc}) \) as an inner product of two functions \( f \) and \( \gamma_n \) on CM-points:
\[ \ell_\chi(f; x_{nc}) = \# O_{cm}(x_{nc})^{-1}(f; \gamma_n). \]
The Hecke operator is certainly self-adjoint for this inner product. Thus we have:

**Corollary 3.3.** Let \( f \) be an eigenform with eigenvalue \( \lambda_m \) under the action by \( T_m \). Then for \( n \) prime to \( c \),
\[ \ell_\chi(f; x_{nc}) = \left( \sum_{m | n} s_\chi(n/m) \lambda_m \right) \cdot \ell_\chi(f; x_c). \]

**Proposition 3.4.** Assume the \( \delta \)-bound in §2. For any \( \epsilon > 0 \), there is an \( C(\epsilon) > 0 \) depending only on \([F : \mathbb{Q}]\) such that
\[ |\ell_\chi(f; x_{nc})| \leq C(\epsilon) N n^{1/2+\delta+\epsilon} |\ell_\chi(f; x_c)|. \]
Proof. The period sum is given by

\[ \ell_\chi(f; x_{nc}) = \prod_{\wp^{n\ell_{\wp}}} \kappa(\wp^e) \cdot \ell_\chi(f; x_c) \]

where

\[ \kappa(\wp^n) = \sum_{i=0}^{e} s_\chi(\pi^{e-i}) \lambda_{\wp^n}. \]

Let’s compute this number in separate cases.

First assume that \( \wp \) is inert in \( K \). Then

\[ s_\chi(\pi^{e-i}) = \begin{cases} 
1 & \text{if } e = i \\
-\chi(\pi) & \text{if } e = i + 2 \\
0 & \text{otherwise}
\end{cases} \]

Here it is understood that \( \chi(\pi) = 1 \) if \( \chi \) is unramified, and that \( \chi(\pi) = 0 \) if \( \chi \) is ramified. It follows that

\[ \kappa(\pi^e) = \lambda_{\wp^n} - \chi(\pi) \lambda_{\wp^n-2}. \]

Here it is understood that \( \lambda_{\wp^n} = 0 \) if \( n < 0 \).

Now let’s treat the case where \( \wp \) is ramified in \( K \). Then

\[ s_\chi(\pi^{e-i}) = \begin{cases} 
1 & \text{if } e = i \\
-\chi(\pi_K) & \text{if } e = i + 1 \\
0 & \text{otherwise}
\end{cases} \]

It follows that

\[ \kappa(\pi^e) = \lambda_{\wp^n} - \chi(\pi_K) \lambda_{\wp^n-1}. \]

Finally let’s treat the case where \( \wp \) is split in \( K_{\wp} \). Then

\[ s_\chi(\pi^{e-i}) = \begin{cases} 
1 & \text{if } e = i \\
-\chi_1(\pi) + \chi_1(\pi)^{-1} & \text{if } e = i + 1 \\
1 & \text{if } e = i + 2 \\
0 & \text{otherwise}
\end{cases} \]

It follows that

\[ \kappa(\pi^e) = \lambda_{\wp^n} - 2\Re(\chi_1(\pi)) \lambda_{\wp^n-1} + \lambda_{\wp^n-2}. \]

15
Assume that the L-function of $\phi$ has parameter $\alpha$. Then $q^{-n/2}\lambda_n$ is the coefficient of the L-series at $q^{-ns}$:

$$(1 - \alpha q^{-s})^{-1}(1 - \alpha^{-1} q^{-s})^{-1}$$

It follows that

$$\lambda_n = q^{n/2} \frac{\alpha^{n+1} - \alpha^{-1-n}}{\alpha - \alpha^{-1}}.$$

From the $\delta$-bound, $|\alpha^{\pm 1}| \leq q^\delta$. Thus we have that

$$|\lambda_n| \leq q^{(1/2 + \delta + \epsilon)n}.$$ 

It follows that in all cases, $\kappa(\pi^e)$ has bound

$$|\kappa(\pi^e)| \leq q^{e(\delta + 1/2 + \epsilon)}.$$

In summary, we have

$$|\ell_x(f; x_{nc})| \leq C(\epsilon) NN^{1/2 + \delta + \epsilon} |\ell_x(f; x_{nc})|.$$

□

4 Period sums

In this section we want to finish the proof of Theorem 2.2. By the equality

$$\ell(f, O(x)) = i(\Gamma)^{-1} \sum_x \ell_x(f; x),$$

the question is reduced to estimating the sum $\ell_x(f; x)$.

Consider the spectral decomposition:

$$(4.1) \quad f = \sum c_n f_n + \int_\Omega c_\mu E_\mu d\mu$$

where the $f_n$ are discrete (cuspidal or residual) eigenforms under Hecke operators with norm 1, and the $E_\mu$ are Eisenstein series indexed by characters $\mu$ of $F^* \backslash A_F^*$ modulo equivalence $\mu \sim \mu^{-1}$, which exist only when $B = M_2(F)$. The measure $d\mu$ is induced from a Haar measure on the topological group of
idele class characters of \( F \). In this case, for discrete spectrum, we may take \( f_n \) to be

\[
f_n = \| f_{new} \|^{-1} f_{new}^n
\]

with \( f_{new}^n \) a newform. For the continuous spectrum, we may take \( E_\mu \) to be

\[
E_\mu = |L(1, \mu^2)|^{-1} E_{\mu}^{new}
\]

where \( E_{\mu}^{new} \) is the newform in \( \pi(\mu, \mu^{-1}) \). Here a new form \( \varphi^{new} \) means a Hecke eigenform with minimal level and normalized so that

\[
L(s, \Pi) = \text{disc}(F)^{1/2-s} \int_{F^{x} \backslash \mathbb{A}_F^x} (\varphi^{new} - C_{\varphi^{new}}) \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} |a|^{1-1/2} d^x a,
\]

where \( \Pi \) is the automorphic representation of \( \text{GL}_2(\mathbb{A}_F) \) generated by \( \varphi^{new} \), and \( C_{\varphi^{new}} \) is the constant part in the Fourier expansion with respect characters of the unipotent group of matrixes \( \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \).

Since \( f \) is compactly support we have

\[
\| f \|^2 = \sum |c_n|^2 + \int_\Omega |c_\mu|^2 d\mu < \infty.
\]

Moreover, for \( \Delta \) the Laplacien operator on \( M_U(\mathbb{C}) \), \( \Delta^m f \) is still compactly supported for any positive integer \( m \),

\[
\| \Delta^m f \|^2 = \sum |c_n \lambda_n^m|^2 + \int_\Omega |c_\mu \lambda_\mu^m|^2 d\mu < \infty
\]

where \( \lambda_i \) (resp. \( \lambda_\mu \)) are eigenvalues of \( f_i \) (resp. \( E_\mu \)) under \( D \). Thus \( c_n \) (resp. \( c_\mu \)) decays faster than any negative power of \( \lambda_n \) (resp. \( \lambda_\mu \)).

It can be shown that \( \| \phi_n \|_{\sup} \) is bounded by a polynomial function of \( \lambda_n \). Thus, the sum of the right hand side of (4.1) are absolutely convergent point-wisely. Similarly, for a fixed a compact domain \( E \) of \( M(\mathbb{C}) \), it can be shown that \( \sup_{x \in E} |E_\mu(x)| \) is bounded by a polynomial function of \( \lambda_\mu \). Thus, the integral of the right hand side of (4.1) are absolutely and uniformly convergent on \( E \). See Clozel-Ullmo [6], Lemma 7.2-7.4 for a complete proof.

It follows that:

\[
\ell(f; x) = \sum c_n \ell(f_n; x) + \int_\Omega c_\mu \ell(E_\mu; x) d\mu.
\]

Thus, for proof of Theorem 2.2, it suffices to show the following:
Proposition 4.1. For any $\epsilon > 0$, there are positive numbers $C$, $A$ such that for any Hecke eigen form $f$ of norm 1 (which is either cuspidal or Eisenstein):

$$|\ell_\chi(f; x)| \leq C \cdot \lambda(f)^A \cdot \text{disc}(x)^{1/4+\delta/2+\epsilon}$$

where $\|f\| = |L(1, \mu^2)|$ if $f \in \pi(\mu, \mu^{-1})$.

Let $c$ be the conductor of $\chi$ and $nc$ be the conductor of $x$. Then by Proposition 3.4

$$|\ell_\chi(f; x)| \ll N(n)^{\delta+1/2+\epsilon} |\ell_\chi(f; x_0)|$$

where $x_0$ is a CM-point of conductor $c$ with the same CM-group. Now the question is reduced to estimating $\ell_\chi(f; x_0)$. In the following, we will show that this special case follows from the central value formula proved in [31, 36] and the subconvexity bound.

By Jacquet-Langlands theory, there is a unique newform $\varphi$ on $GL_2(\mathbb{A}_F)$ of weight 0 and level $N$ which has the same Hecke eigenvalues as $f$. Notice that when $N = \mathcal{O}_F$, $B = M_2(F)$ and $\varphi$ is a multiple of $f$.

Theorem 4.2 ([31, 36]). Let $\chi$ be a character of $T(\mathbb{Q}) \backslash T(\hat{\mathbb{Q}})$ with the same conductor as $x$.

$$L(1/2, \Pi \otimes \chi) = \frac{2^{[F:Q]+d}}{\sqrt{\text{disc}(x_0)}} \cdot \|\varphi\|^2 \cdot |\ell_\chi(f; x_0)|^2.$$

Here $L(s, \Pi \otimes \chi)$ is the Rankin-Selberg convolution of $L(s, \Pi)$ and $L(s, \chi)$.

Proof. When the conductor $c$ of $\chi$ is prime to the relative discriminant $d$ of $K$, this is proved in [36]. For Eisenstein series $\Pi$ without coprime condition $(c, D) = 1$, this can be proved easily by the same method in [36]. For cusp form $\Pi$ without coprime condition $(c, d) = 1$, the formula can be deduced from Waldspurger’s formula in [31], prop 7, Page 222.

Now Proposition 4.1 for $x = x_0$ follows from Theorem 4.2 and following well known estimate:

$$\lambda(f)^\varepsilon \gg \|\varphi\| \gg \lambda(f)^{-\varepsilon}$$

for $\lambda$ big and any $\varepsilon > 0$. 

18
5 Galois orbits

In this section, we are going to prove Theorem 2.5 about an estimate of the sizes of Galois orbits CM-points with maximal Mumford-Tate group, provided the \( \epsilon \)-conjecture on class groups.

Let \( x \) be a CM-point with CM-group \( T = K^\times / F^\times \) and Mumford-Tate group \( H \subset T \). By the Shimura theory, the CM orbit \( O_{cm}(x) \) as a reduced subscheme is defined over the reflex field \( \tilde{K} \subset C \) generated over \( \mathbb{Q} \) by \( \sum_{\sigma \in S_K} \sigma(x) \) for all \( x \in F \). Moreover the Galois action is given by a homomorphism

\[
(5.1) \quad r_x : \text{Gal}(\overline{\mathbb{Q}}/\tilde{K}) \longrightarrow K^\times \backslash \tilde{K}^\times / \tilde{F}^\times \tilde{O}_x^\times = \text{Pic}(O_x)/\text{Pic}(O_F)
\]

where \( O_x \) is the order of \( x \) defined in \S 2.

The Galois action factors through the maximal abelian quotient, thus is determined by the homomorphism

\[
\tilde{K}^\times \tilde{\longrightarrow} K^\times \tilde{\longrightarrow} \tilde{O}_x^\times.
\]

By Shimura’s theory this is induced by a homomorphism of algebraic groups

\[
N : \tilde{K}^\times \longrightarrow K^\times, \quad \tau N(x) = \prod_{\tau \in \sigma \in S_K} \sigma(x)
\]

where \( \tau \) is a any fixed embedding \( K \longrightarrow \mathbb{C} \), and \( \sigma \) runs through the coset \( \text{Gal}(\mathbb{C}/\mathbb{Q})/\text{Gal}(\mathbb{C}/\tilde{K}) \). Notice that the definition does not depend on the choice of \( \tau \). The restriction of \( N \) to the totally real subgroup \( \tilde{F}^\times \) takes values in \( F^\times \). Thus \( N \) induces a homomorphism on the quotient which also denoted by \( N \):

\[
N : \tilde{T} := \tilde{K}^\times / \tilde{F}^\times \longrightarrow T = K^\times / F^\times.
\]

Let \( F_0 \) be the subfield of \( F \) over which all embeddings of \( S \) have the same restriction. Then \( K^\times / F^\times \) and \( \tilde{K}^\times / \tilde{F}^\times \) can be viewed as algebraic groups \( T_0 \) and \( \tilde{T}_0 \) over \( F_0 \), and the morphism \( N \) is induced by a morphism over \( F_0 \):

\[
(5.2) \quad N_0 : \tilde{T}_0 \longrightarrow T_0.
\]

The assumption that \( H = T \) means that \( N_0 \) is surjective. Taking \( L \) to be a Galois closure of \( K \) over \( F_0 \), these groups are split over \( L \). First we want to show that \( N_0 \) has a section up to isogeny.
Lemma 5.1. Let $\alpha : T_1 \to T_2$ be a surjective homomorphism of tori over $F_0$ which are split over $L$. Let $n$ be a positive integer which is a product of $[L : F_0]$ and an integer $m$ annihilating the components group of $\ker \alpha$. Then there is a homomorphism $\beta : T_2 \to T_1$ such that $\alpha \circ \beta = n$ on $T_2$.

Proof. Let $\alpha^* : X(T_2) \to X(T_1)$ be the corresponding injection of $\text{Gal} \mathbb{Q}/F_0$-modules of characters. It suffices to show that there is a homomorphism of $\text{Gal} \mathbb{Q}/F_0$-modules $\phi : X(T_1) \to X(T_2)$ such that $\alpha^* \circ \phi = n$. Since both $T_i$ are split over $L$, the $\text{Gal} \mathbb{Q}/F_0$-module structures on $X(T_i)$ descend to $\Delta$-module structures, where $\Delta = \text{Gal}(L/F_0)$. Let $X(T_1) = Y_1 + Y_2$ be a direct sum decomposition of $\mathbb{Z}$-modules such that $Y_2$ is the subgroup of elements $x$ such that some positive multiple $mx \in X(T_2)$. Then $Y_2$ is a $\Delta$-submodule and $Y_2/X(T_2)$ is annihilated by $n$. Let $\pi' \in \text{End}(X(T_1))$ denote the projection of $X(T_1)$ onto $Y_1$ with respect to this decomposition and let

$$\pi := m \cdot \sum_{\delta \in \Delta} \delta^{-1} \circ \pi' \circ \delta.$$ 

Then $\pi$ is $\Delta$-homomorphism with values in $X(T_2)$, and for $x \in X(T_2)$, $\pi(x) = nx$.

Corollary 5.2. Let $n$ be the product of $[L : F_0]$ and the smallest positive integer annihilating the components group of $\ker N_0$. The cokernel of $r_x$ is annihilated by $n$.

Proof. By Lemma 5.1, $N_0$ will have a section up to multiplication by $n$. Thus for any $F_0$-algebra $A$, the morphism on any $A$-points of $T_i$ will have cokernel annihilated by $n$.

Proof of Theorem 2.5 The corollary implies that the image of the homomorphism $r_x$ in (5.1) has order bounded below by

$$\frac{\#(\text{Pic} O_x/\text{Pic} F)}{\#(\text{Pic} O_x/\text{Pic} F)[n]}.$$ 

Now Theorem 2.5 follows from the Brauer-Siegel estimate

$$\#\text{Pic}(O_x) \gg \text{disc}(x)^{1/2-\epsilon}.$$ 

20
In the rest of section, we want to estimate $\ell$-torsion in the anticyclotomic extension in two special cases. For an abelian group $M$ and prime $\ell$, let $\text{rank}_\ell$ denote the $\ell$-rank of $M$:

$$\text{rank}_\ell M := \text{rank}_{\mathbb{Z}/\ell\mathbb{Z}} M \otimes \mathbb{Z}/\ell\mathbb{Z} = \text{rank}_{\mathbb{Z}/\ell\mathbb{Z}} M[\ell].$$

It is easy to see that $\text{rank}_\ell M$ is the minimal number of generators for the $\ell$-Sylow subgroup of $M$.

**Proposition 5.3.** Let $O_c = O_F + cO_K$ be an order of a CM-field $K$, where $F$ is its totally real subfield.

1. Let $\mu$ be the number of prime factors of $c$. Consider the map

$$\alpha : \text{Pic}(O_c) \longrightarrow \text{Pic}(O_K).$$

Then

$$\text{rank}_\ell \ker(\alpha) \leq g\mu.$$  

2. Let $\delta$ be the number of primes of $O_K$ ramified over $F$, then

$$\text{rank}_2(\text{Pic}(O_K)) \leq 2 \text{rank}_2(\text{Pic}O_F) + g + \delta.$$  

**Proof.** It is easy to see that $\ker \alpha$ has an expression

$$\ker \alpha = \hat{O}_K^\times / O_K^\times \cdot \hat{O}_K^\times = (O_k/c)^\times / O_K^\times (O_F/c)^\times.$$

Thus $\text{rank}_\ell \ker \alpha$ is additive over prime decomposition of $c$. So we need only to estimate the $\text{rank}_\ell \ker \alpha$ for $c = \pi^n$ a positive power of prime $\pi$ of $O_F$. Consider the exact sequence

$$1 \longrightarrow \frac{1 + \pi O_K}{1 + \pi O_F + \pi^n O_K} \longrightarrow \frac{(O_K/\pi^n)^\times}{(O_F/\pi^n)^\times} \longrightarrow \frac{(O_K/\pi)^\times}{(O_F/\pi)^\times} \longrightarrow 1.$$  

This induces an exact sequence

$$1 \longrightarrow \frac{1 + \pi O_K}{1 + \pi O_F + \pi^n O_K}[\ell] \longrightarrow \frac{(O_K/\pi^n)^\times}{(O_F/\pi^n)^\times}[\ell] \longrightarrow \frac{(O_K/\pi)^\times}{(O_F/\pi)^\times}[\ell].$$  

If the characteristic of $O_F/\pi$ is not $\ell$ (resp. $\ell$), the $\ell$-rank of the first group is 0 (resp. bounded by $g$) while the last group is group is bounded by 1 (resp. 0). Thus

$$\text{rank}_\ell \left( \frac{(O_K/\pi^n)^\times}{(O_F/\pi^n)^\times} \right) \leq g.$$  

21
This proves the first part.

Now we assume that $\mathcal{O}_c = \mathcal{O}_K$ and let $\xi \in \text{Pic}(\mathcal{O}_K)[2]$ be a class. Then we have the homomorphism

$$\beta : \text{Pic}(\mathcal{O}_K) \longrightarrow \text{Pic}(\mathcal{O}_F) \quad \beta(\xi) = \xi \cdot \bar{\xi}.$$ 

Thus

$$\text{rank}_2(\text{Pic}\mathcal{O}_K) \leq \text{rank}_2(\text{Pic}\mathcal{O}_F) + \text{rank}_2 \ker \beta.$$ 

Now assume that $\xi \in \ker \beta$. Then both $\xi^2, \xi \bar{\xi}$ are trivial, and so is $\xi/\bar{\xi}$. Let $\xi$ be represented by an $x \in \hat{K}^\times$:

$$\text{Pic}(\mathcal{O}_K) = \hat{K}^\times/K^\times \hat{\mathcal{O}}_K^\times.$$ 

Then we have an expression:

$$(5.3) \quad x/\bar{x} = tu, \quad t \in K^\times, \quad u \in \hat{\mathcal{O}}_K^\times.$$ 

Taking norm $N_{K/F}$ on both sides, we find that $N(t) \in \mathcal{O}_F^\times$. As $t$ is uniquely determined modulo $\mathcal{O}_K^\times$, the norm $N_{K/F}(t) \in \mathcal{O}_F^\times$ is uniquely determined modulo $N(\mathcal{O}_K^\times)$. Thus we have homomorphism

$$\gamma : \ker \beta \longrightarrow \mathcal{O}_F^\times/N_{K/F}(\mathcal{O}_K^\times).$$

As $(\mathcal{O}_F^\times)^2 \subset N(\mathcal{O}_K)$, the second group has 2-rank bounded by $g$. Thus we have

$$\text{rank}_2 \ker \beta \leq g + \text{rank}_2 \ker \gamma.$$ 

Now we assume that $\xi \in \ker \gamma$. Then may take $t \in K^\times$ so that $N_{K/F}(t) = 1$. By Hilbert 90, there is an $s \in \hat{K}^\times$ such that $t = \bar{s}/s$. Now replacing $x$ by $sx$ which does not change the class of $\xi$, we may assume that $t = 1$ in the expression in (5.3). Let $I$ denote the elements in $\hat{K}^\times$ which are invariant under conjugation modulo $\hat{\mathcal{O}}_K^\times$. Then we have

$$\ker \gamma = I/(I \cap K^\times)\hat{\mathcal{O}}_K^\times[2].$$

Now we consider the homomorphism

$$\theta : \ker \gamma \longrightarrow I/\hat{F}^\times(\hat{I} \cap K)^\times \hat{\mathcal{O}}_K^\times.$$ 

As the second group is a quotient of the genus group of $K$ and generated by ramified primes of $\mathcal{O}_K$, we have

$$\text{rank}_2 \ker \gamma = \text{rank}_2 \ker \theta + \delta.$$ 

22
where $\delta$ is number of ramified primes of $\mathcal{O}_K$ over $\mathcal{O}_F$.

It remains to estimate $\ker \theta$, which is certainly a quotient of $\text{Pic}(\mathcal{O}_F)$. It follows that

$$\text{rank}_2 \ker \theta \leq \text{rank}_2(\text{Pic}(\mathcal{O}_F)).$$

\[\square\]

**Corollary 5.4.** Let $n$ be a fixed positive integer with decomposition $n = 2^t m$ with $m$ odd. Then for any $\epsilon > 0$,

$$\#\text{Pic}\mathcal{O}_c[n] \ll \text{disc}(\mathcal{O}_c)^\epsilon \cdot \#\text{Pic}(\mathcal{O}_K)[m].$$

**Proof.** Consider the morphism $\alpha : \text{Pic}(\mathcal{O}_c) \longrightarrow \text{Pic}(\mathcal{O}_K)$. Then we have

$$\#\text{Pic}\mathcal{O}_c[n] \leq \#\text{Pic}(\mathcal{O}_K)[n] \cdot \#\text{Ker} \alpha[n]$$

$$= \#\text{Pic}(\mathcal{O}_K)[m] \cdot \#\text{Pic}(\mathcal{O}_K)[2^t] \cdot \#\text{Ker} \alpha[n].$$

It remains to estimate the last two terms. Write $n = \prod p_i^{n_i}$.

$$\#(\text{Pic}\mathcal{O}_K)[2^t] \leq 2^{t \text{rank}_2 \text{Pic}\mathcal{O}_K} \leq 2^{t(2 \text{rank}_2 \mathcal{O}_F + \delta)} \ll \text{disc}(\mathcal{O}_K)^\epsilon.$$  

$$\#\text{Ker} \alpha[n] \leq \prod_i p_i^{n_i \cdot \text{rank}_p \text{Ker} \alpha} \leq n^{g \mu} \ll N(c^2)^\epsilon.$$

\[\square\]

6 Mumford-Tate groups

In this section we will compute the Mumford-Tate group for CM-points on $M_U$. When $d = 1$ or 2, our result is complete. When $d > 2$, we will give some examples where every CM-point has maximal Mumford-Tate group.

Let us fix a CM-type $(K,S_K)$. Let $\Sigma_K$ denote the set of all complex $\sigma_0$-embeddings of $K$ which admit an action by $\text{Gal}(\overline{\mathbb{Q}}/F_0)$ by composition. The character group of the algebraic torus $K^\times$ over $F_0$ is the group $\mathbb{Z}[\Sigma_K]$ of divisors on $\Sigma_K$ with left action. We may also view $\mathbb{Z}[\Sigma_K]$ as the space of functions $\phi$ on $\Sigma_K$ under the correspondence:

$$\phi \longrightarrow \sum_{\sigma \in \Sigma_K} \phi(\sigma)[\sigma].$$

23
With this convention, the group of characters of the CM-group $T_0 = K^\times / F^\times$ is the Galois submodule $\mathbb{Z}[\Sigma]^-\sigma_0$ of functions annihilated by $1 + [c]$ where $c$ is complex conjugation acting on $\Sigma_K$. Let $\Sigma_{\bar{K}}$ denote the set of all complex $\sigma_0$-embeddings of $\bar{K}$ equipped with action by $\text{Gal}(\bar{Q}/F_0)$. Then $\Sigma_{\bar{K}}$ can be identified with the set
\[
\{gS_K, \quad g \in \text{Gal}(\bar{Q}/F_0)\}
\]
of subsets of $\Sigma_K$. Again the groups of characters of the torus $\tilde{T} := \tilde{K}^\times / \tilde{F}^\times$ can be identified with $\mathbb{Z}[\Sigma_{\bar{K}}^-\sigma_0]$. Recall that we have a norm morphism
\[
(6.1) \quad N_0 : \tilde{T}_0 \longrightarrow T_0, \quad \tau N_0(x) = \prod_{\tau \in \sigma \circ S_K} \sigma(x)
\]
for any $\tau \in \Sigma_K$. The Mumford-Tate group $H$ is the restriction of scalars of the image $H_0$ of $N_0$. Let $N_0^*$ denote the induced homomorphism of Galois modules of characters:
\[
N_0^* : \quad \mathbb{Z}[\Sigma_K]^- \longrightarrow \mathbb{Z}[\Sigma_{\bar{K}}]^-.
\]

**Proposition 6.1.** With notation as above, we have the following assertions:

1. For any $\phi \in \mathbb{Z}[\Sigma_K]^-\sigma_0$,
\[
N_0^*(\phi)(gS) = \sum_{\sigma \in S_K} \phi(gs).
\]

2. Let $\Phi = \ker N_0^*$. The group of characters of the Mumford-Tate group $H_0$ is
\[
X(H_0) = \mathbb{Z}[\Sigma_K]/\Phi.
\]

3. The order of the component group of $\ker N_0$ is bounded by a constant independent of $K$ and $S_K$.

4. Let $p$ be a prime. Then $p$ does not divide the component group of $\ker N_0$ if and only if
\[
\ker(N_0^* \otimes \mathbb{F}_p) = (\ker N_0^*) \otimes \mathbb{F}_p.
\]
Proof. The first assertion follows from a direct computation:

\[ N_0^* \phi = \phi \circ N_0 = \sum_{g \in \Sigma_K} \phi(\sigma) \sum_{s \in g \circ S_K} [gS_K] = \sum_{g \in \Sigma_K} \left( \sum_{s \in S_K} \phi(gs) \right) [gS_K]. \]

The second assertion follows from the decomposition of \( N_0 \)

\[ \tilde{T}_0 \rightarrow H \rightarrow T_0 \]

which induces a decomposition of the character groups

\[ X(T_0) \rightarrow X(H_0) \rightarrow X(T_0). \]

The third assertion follows from the fact that the group of components of \( \ker N_0 \) is dual to the maximal torsion subgroup of \( \operatorname{Coker}N_0^* \) and the fact that there are only finitely many isomorphic classes of homomorphism \( N_0^* \) of \( \mathbb{Z} \)-modules.

For the last assertion, we notice that \( p \) does not divides the order of the component group if and only if the induced homomorphism

\[ X(H_0) \otimes \mathbb{F}_p \rightarrow X(\tilde{T}_0) \otimes \mathbb{F}_p \]

remains injective. This is equivalent to the following identity

\[ X(H_0) \otimes \mathbb{F}_p = \mathbb{F}_p[\Sigma_K]/\ker(N_0^* \otimes \mathbb{F}_p), \]

which is equivalent to

\[ (\ker N_0^*) \otimes \mathbb{F}_p = \ker(N_0^* \otimes \mathbb{F}_p). \]

In the following we want to compute \( H_0 \) in some special cases. The case where \( M_U \) has dimension 1 is easy:

**Proposition 6.2.** If \( S_K \) consists a single element then \( \tilde{K} = K \), \( H = T \) and the reciprocity map \( N_0^* : \tilde{T}_0 \rightarrow T_0 \) is the identity map.

Now we consider the case where \( S_K \) has two elements.
Proposition 6.3. Assume that the set $S_K$ consists of two elements $\sigma_1, \sigma_2$. Let $K_0$ (resp. $F_0$) be the subfield of $K$ (resp. $F$) consisting of elements $x$ such that $\sigma_1(x) = \overline{\sigma_2(x)}$. Then the torus $H_0$ is isomorphic to the kernel of the norm map
\[ N_{K/K_0} : \quad K^\times/F^\times \longrightarrow K_0^\times/F_0^\times. \]
Moreover the kernel of the morphism
\[ N_0 : \quad \tilde{T}_0 \longrightarrow T_0 \]
is connected.

Proof. Let us fixed an embedding of $K$ into $\mathbb{C}$ by the element $\sigma_1$ in $S_K$ and let $L$ be a Galois closure of $K$ over $F_0$ in $\mathbb{C}$. Write $\Delta = \text{Gal}(L/F_0)$ and $\Delta_M = \text{Gal}(L/M)$ for an extension $M$ of $F_0$ in $L$. Then we have inclusions:
\[ \Delta \supset \Delta_F = (\Delta_K, c) \supset \Delta_K \]
where $c \in \Delta$ is complex conjugation. The set $\Sigma_K$ is naturally identified with the cosets $\Delta/\Delta_K$. We lift $\sigma_1, \sigma_2 \in S_K$ to $e, s \in \Delta$ respectively. Then $\Delta$ is generated by $\Delta_F$ and the set $s$.

With above notations, $\mathbb{Z}[\Sigma_K]$ can be identified with the set of functions on $\Delta$ right invariant by $\Gamma_K$ and with eigenvalue $-1$ under $c$. The space $\Phi$ in proposition 6.1 becomes the space of functions with the above property and such that
\[ \phi(g) + \phi(gs) = 0, \quad \forall g \in \Delta \]
or equivalently
\[ \phi(g) = \phi(gcs). \]
This is equivalent to saying that $\phi$ is invariant under the subgroup $(\Delta_K, sc) = \Delta_{K_0}$. Then $\Phi$ is the subspace of functions on $\Delta$ invariant by $\Delta_{K_0}$ and having eigenvalue $-1$ under $c$. Thus $\Phi$ is the character group of $K_0^\times/F_0^\times$.

On the other hand the exact sequence
\[ 1 \longrightarrow \ker N_{K/K_0} \longrightarrow K^\times/F^\times \longrightarrow K_0^\times/F_0^\times \longrightarrow 1 \]
induces a morphism of groups of characters
\[ 1 \longrightarrow X(K_0^\times/F_0^\times) \longrightarrow X(K^\times/F^\times) \longrightarrow X(\ker N_{K/K_0}) \longrightarrow 1. \]
If we identified the first two groups of characters as functions on $\Delta$ invariant under right translation by $\Delta_{K_0}$ and $\Delta_K$ respectively, then the map is the
natural inclusion. Thus we have shown that $X(H) = X(\ker N_{K/K_0})$. It follows that $H = \ker N_{K/K_0}$.

To show that $N_0$ has connected kernel, we want to verify part 3 of Proposition 6.1. Notice that $\ker(N_0^* \otimes \mathbb{F}_p)$ is the set of $\mathbb{F}_p$-valued functions $\psi$ satisfying

$$\psi(g) + \psi(gs) = 0.$$ 

The same proof as above shows that this equivalent $\psi$ being invariant under $\Delta_{K_0}$ and having eigenvalue $-1$ under $c$. Thus $\psi$ is a reduction of a $\mathbb{Z}$-valued function invariant under $\Delta_{K_0}$. Thus the equality of part 4 of Proposition 6.1 holds.

\begin{proof}

Remarks

1. If $K_0 = F_0$, then $H = T$.
2. If $K_0 \neq F_0$ then $K = K_0 \cdot F$.
3. Conversely, let $K_0$ be an imaginary quadratic extension of $F_0$ and take $K = K_0 \cdot F$. There always exists a lifting of $S$ to $S_K$ such that $K_0$ is not fixed by the elements $\sigma_1, \sigma_2$ in $S_K$. Then $K_0$ must fixed by $\sigma_1, c\sigma_2$. By Proposition 6.3, $H$ is the kernel of $K^x/F^x \longrightarrow K_0^x/F_0^x$.

It seems hard to write a general description of the Mumford-Tate groups for any quaternion Shimura variety of dimension 3 or higher. In the following, we give a statement for cases where

- every CM-point has maximal Mumford-Tate group.
- the subconvexity bound and $\epsilon$ conjecture imply the equidistribution of Galois orbits of CM-points.

Proposition 6.4. Let $\Sigma$ be the set of $\sigma_0$-embeddings of $F$ equipped with a natural action by $\text{Gal}(\bar{\mathbb{Q}}/F_0)$. Assume that there is no nonzero function

$$\psi: \Sigma \longrightarrow \mathbb{F}_2 := \mathbb{Z}/2\mathbb{Z}$$

such that

$$\sum_{s \in S} \psi(gs) = 0, \quad \forall g \in \text{Gal}(\bar{\mathbb{Q}}/F_0).$$

Then for any CM-point on $M_U$, $H = T$.

\begin{proof}

The reduction (mod 2) of any $\phi \in \Phi$ will be invariant under complex conjugation and thus define a $\mathbb{F}_2$-valued function on $\Sigma$. The assumption then implies that $\phi \equiv 0 \mod 2$. Thus $\Phi/2\Phi = 0$ and then $\Phi = 0$. \hfill $\square$

\end{proof}
We may apply the proposition when $F/F_0$ is abelian:

**Proposition 6.5.** Assume that $F/F_0$ is abelian with Galois group $\Gamma$ satisfying that there is no character $\chi: \Gamma \rightarrow \mathbb{F}_2^\times$ such that

$$\sum_{s \in S} \chi(s) = 0.$$ 

Then for any CM-point on $M_U$, $H = T$.

**Proof.** We want to show that the condition of Proposition 6.4 is satisfied. The proof is divided into two steps. In the first step, we reduce the proof to the case where $\#\Gamma$ is odd. Then we prove the lemma when $\#\Gamma$ is odd.

Without loss of generality, we assume that $e \in S$. Then the equation in the Proposition gives

$$\psi(g) = \sum_{s \neq e} \psi(gs), \quad \forall g \in \Gamma.$$ 

Taking this equation with $g$ replaced by $gs$, we then obtain

$$\psi(g) = \sum_{s \neq 1, t \neq 1} \psi(gst) = \sum_{s \neq 1} \psi(gs^2).$$ 

We may repeat this steps to obtain

$$\psi(g) = \sum_{s \neq 1} \psi(gs^{2^n})$$

for any $n \in \mathbb{N}$. Let $\Gamma = \mathbb{Z}/2m \times \Gamma'$ be the decomposition of $\Gamma$ with $\Gamma'$ a commutative group of odd order. Take an $n$ so that $g \rightarrow g^{2^n}$ is the projection $\Gamma \rightarrow \Gamma'$. Let $S'$ be the set of elements in $\Gamma'$ whose preimage in the projection $S \rightarrow \Gamma'$. For any $h \in \Gamma$, the function $\psi_h(g') := \psi(gh)$ ($g' \in \Gamma$) will satisfy the equation

$$\sum_{s \in S'} \psi_h(g's') = 0, \quad \forall g' \in \Gamma'.$$

Thus we are reduced to proving that $\psi_h = 0$ on $\Gamma'$ for all $h$. Since $S'$ also has odd cardinality, we are in the case where $\Gamma$ is odd.
Assume that $\Gamma$ is odd. Let $\Psi$ be the space of functions $\psi$ on $\Gamma$ satisfying the equation in the Lemma. Then $\Psi \otimes \overline{F}_2$ will be a direct sum of characters. Thus we need to show that there is no character $\chi : \Gamma \to \overline{F}_2^\times$ such that

$$\sum_{s \in S} \chi(s) = 0.$$ 

\[ \square \]

**Corollary 6.6.** Assume that $\# S$ is odd, and that $F$ is abelian over $F_0$ such that the order of $\text{Gal}(F/F_0)$ is a power of 2. Then $H = T$ for every CM-point on $M_U$.

We have some further statements for abelian case.

**Proposition 6.7.** Assume that $F$ is abelian over $F_0$ with Galois group $\Gamma$ such that the following conditions are verified:

1. $\Gamma$ has cyclic $2$-primary part $\Gamma[2^\infty]$;
2. for all character $\alpha : \Gamma \to \mu_{p^n}$ of order a positive power of an odd prime $p$, $\alpha(S)$ does not contain any coset of $\mu_p$.

Then $H = T$ for any CM-point on $M_U$.

**Corollary 6.8.** Assume the following conditions are verified:

1. $\# S$ is odd and $< p$ for all odd prime factor $p$ of $[F : F_0]$;
2. the Galois group $\text{Gal}(F/F_0)$ is commutative with cyclic $2$-primary $2$.

Then $H = T$ for every CM-point on $M_U$.

**Proof of Proposition 6.7.** Let us fix an embedding of $K$ into $\mathbb{C}$ by an element in $S_K$, and let $L$ be a Galois closure of $K$ over $F_0$ in $\mathbb{C}$. Write $\Delta = \text{Gal}(L/F_0)$ and $\Lambda = \text{Gal}(L/F)$, $\Lambda_K = \text{Gal}(L/K)$ then we have inclusions:

$$\Delta \supset \Lambda = (\Lambda_K, c) \supset \Lambda_K$$

where $c \in \Delta$ is complex conjugation. The following lemma gives an almost commutative lifting of $\Gamma$:
Lemma 6.9. Consider an exact sequence of finite groups:

\[ 1 \longrightarrow \Lambda \longrightarrow \Delta \longrightarrow \Gamma \longrightarrow 1. \]

Assume the following properties are satisfied:

1. \( \Gamma \) is commutative and fits in an exact sequence:

\[ 1 \longrightarrow \Gamma_2 \longrightarrow \Gamma \longrightarrow \Gamma_1 \longrightarrow 1 \]

so that one of \( \Gamma_i \) is odd and one is 2-primary and cyclic.

2. \( \Lambda \) is commutative and has order a power of 2.

Then \( \Delta \) contains a commutative subgroup \( \tilde{\Gamma} \) mapping surjectively onto \( \Gamma \).

Proof. Indeed, the extension

\[ 0 \longrightarrow \Lambda \longrightarrow \Delta \longrightarrow \Gamma \longrightarrow 0 \]

is given by an element \( \xi \in H^2(\Gamma, \Lambda) \) which can be computed using the spectral sequence \( H^i(\Gamma_1, H^j(\Gamma_2, \Lambda)) \). As \( \Lambda \) has order a power of 2, the cohomology of odd groups vanish. Thus we have

\[
H^2(\Gamma, \Lambda) = \begin{cases} 
H^2(\Gamma_1, H^0(\Gamma_2, \Lambda)) & \text{if } \Gamma_2 \text{ is odd} \\
H^0(\Gamma_1, H^2(\Gamma_1, \Lambda)) & \text{if } \Gamma_1 \text{ is odd}
\end{cases}
\]

Notice that the \( H^2 \) cohomology of a cyclic group is equal to Tate’s cohomology group \( \hat{H}^0 \). Thus we have

\[
H^2(\Gamma, \Lambda) = \begin{cases} 
\hat{H}^0(\Gamma_1, H^0(\Gamma_2, \Lambda)) & \text{if } \Gamma_2 \text{ is odd} \\
H^0(\Gamma_1, \hat{H}^0(\Gamma_2, \Lambda)) & \text{if } \Gamma_1 \text{ is odd}
\end{cases}
\]

\[
= \begin{cases} 
H^0(\Gamma, \Lambda)/N_{\Gamma_2}H^0(\Gamma_2, \Lambda) & \text{if } \Gamma_2 \text{ is odd} \\
H^0(\Gamma, \Lambda)/N_{\Gamma_1}H^0(\Gamma_1, \Lambda) & \text{if } \Gamma_1 \text{ is odd}
\end{cases}
\]

where \( N_{\Gamma_i} \) is the norm defined by \( \Gamma_i \). Let \( x \) be the element in \( H^0(\Gamma, \Lambda) \) representing \( \xi \). Then there is commutative subgroup \( \tilde{\Gamma} \) of \( \Delta \) which maps surjectively onto \( \Gamma \) with kernel \( X \) generated by \( x \). \( \square \)
The set $\Sigma_K$ is naturally identified with the cosets $\Delta/\Lambda_K$. We pick up liftings of $S_K \subset \Sigma_K$ to $S_L \subset \tilde{\Gamma}$ containing the unit element:

$$e \in S_L \simeq S_K \simeq S.$$ 

Then $\Delta$ is generated by $\Lambda$ and the set $S_L$.

With above notations, $\mathbb{Z}[\Sigma_K]$ can be identified with the set of functions on $\Delta$ invariant under the right by $\Lambda_K$ and with eigenvalue $-1$ under $c$. The space $\Phi$ in proposition 6.1 becomes the space of functions with the above property and such that

$$(6.2) \quad \sum_{\sigma \in S_L} \phi(g\sigma) = 0, \quad \forall g \in \Delta.$$ 

Since $\Delta$ is generated by $S_L$ and $\Lambda$ and $\Lambda$ is normal in $\Delta$, we have an expression

$$\Delta = \tilde{\Gamma} \cdot \Lambda_K.$$ 

Thus the restriction on $\tilde{\Gamma}$ defines injections,

$$\mathbb{Z}[\Delta/\Lambda_K] \longrightarrow \mathbb{Z}[\tilde{\Gamma}], \quad \Phi \longrightarrow \tilde{\Phi},$$

where $\tilde{\Phi}$ is the set of elements in $\mathbb{Z}[\tilde{\Gamma}]$ satisfying the same equation (6.2). Since $\tilde{\Gamma}$ is abelian, $\tilde{\Phi} \otimes \mathbb{C}$ is generated by characters. Now we apply the following lemma to complete the proof of Proposition 6.7:

**Lemma 6.10.** Let $\Gamma$ be a finite commutative group and let $W$ be a subset of $\Gamma$ of odd order. Assume that for each nontrivial character $\alpha : \Gamma \rightarrow \mu_p$, whose order is a power of an odd prime, the image of $W$ does not contain any coset of $\mu_p$. Then there is no character $\chi$ of $\Gamma$ satisfying the equation

$$\sum_{w \in \Gamma} \chi(w) = 0.$$ 

**Proof.** First we want to reduce the proof to the case where $\Gamma$ has no prime bigger than $\#W$.

Let $p$ be an odd prime dividing $\#\Gamma$. Let $\chi$ be a character on $\Gamma$ which has decomposition $\chi = \chi_1 \cdot \chi_2$ into characters with orders prime to $p$ and a power of $p$ respectively. Let $\Gamma_i = \ker \chi_i$, then $\Gamma/\ker \chi = \Gamma_1 \cdot \Gamma_2$. The equation in the Proposition becomes

$$0 = \sum_{w \in W} \chi(w) = \sum_{\zeta \in \chi_2(W)} \phi(\zeta, \chi_1) \zeta,$$
where
\[ \phi(\zeta, \chi_1) = \sum_{w \in W_\zeta} n_\zeta(w)\chi_1(w) \]
and where \( W_\zeta \) is the projection of \( \chi_2^{-1}(\zeta) \cap W \) onto \( \Gamma_1 \), and \( n_\zeta(w) \in \mathbb{N} \) such that
\[ \sum_{\zeta} \sum_{w \in W_\zeta} n_\zeta(w) = \#W. \]

Let \( K \) be the cyclotomic field generated by values of \( \phi(\delta, \chi_1) \). Then \( K \) is disjoint with the field generated by \( \chi_2 \). If \( \chi_2 \) is nontrivial, then the above equation implies that
\[ \phi(\zeta, \chi_1) = \phi(\zeta \eta, \chi_1), \quad \forall \eta \in \mu_p. \]

If one of the \( \phi(\zeta, \chi_1) \neq 0 \), then \( \chi_2(W) \) contains a coset of \( \mu_p \) which contradicts the assumption of the lemma.

By induction on the number of odd prime factors of \( \#\Gamma \), we reduce to the case where \( \#\Gamma = 2^n \) is a power of 2, and the equation is
\[ \sum_{w \in W} n(w)\chi(w) = 0, \]
where \( n(w) \in \mathbb{N} \) such that \( \sum n(w) \) is odd. This is impossible as the only nontrivial relation among \( 2^n \)-th root (like \( \chi(w) \)) of unity is \( \zeta + (-\zeta) = 0. \) \( \Box \)

References


[3] Brumer, Armand; Silverman, Joseph H. The number of elliptic curves over \( \mathbb{Q} \) with conductor \( N \). Manuscripta Math. 91 (1996), no. 1, 95–102


33

[17] Harcos, G; Michel, P; The subconvexity problem for Rankin/Selberg L-functions and equidistributions of Heegner points, II. Preprint 2004

[18] Helfgott, H; Venkatesh, A. Integral points on elliptic curves and 3-torsion in class groups, math.NT/0405180, submitted


